

2/5/1 (Item 1 from file: 351)
DIALOG(R)File 351:DERWENT WPI
(c) 2000 Derwent Info Ltd. All rts. reserv.

012070618 **Image available**
WPI Acc No: 98-487529/199842
XRPX Acc No: N98-381072

Authentication method for encrypted communication system - involves generating first and second authentication information based on random number, confidential information, predefined algorithm which are compared to authenticate validity of first station

Patent Assignee: OKI ELECTRIC IND CO LTD (OKID)

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
JP 10210023	A	19980807	JP 9712876	A	19970127	H04L-009/08	199842 B

Priority Applications (No Type Date): JP 9712876 A 19970127

Patent Details:

Patent	Kind	Lan	Pg	Filing Notes	Application	Patent
JP 10210023	A		42			

Abstract (Basic): JP 10210023 A

The method involves storing common confidential information (Ka,K'a) in memories (13,43), respectively for each station. A first station transmits an information 'Ia'. Either the first or a second station generates a random number 'r' and transmits to other station. The first station generates a first authentication information based on the random number, confidential information and a predetermined algorithm.

Similarly, the second station generates a second authentication information based on random number, confidential information and predetermined algorithm. The second station then compares both the first and second authentication information and authenticates the information generated at the first station.

ADVANTAGE - Prevents tapping in case of separate communication. Eliminates using communicated information again.

Dwg.1/20

Title Terms: AUTHENTICITY; METHOD; ENCRYPTION; COMMUNICATE; SYSTEM;
GENERATE; FIRST; SECOND; AUTHENTICITY; INFORMATION; BASED; RANDOM; NUMBER
; CONFIDE; INFORMATION; PREDEFINED; ALGORITHM; COMPARE; AUTHENTICITY;
VALID; FIRST; STATION

Derwent Class: W01

International Patent Class (Main): H04L-009/08

International Patent Class (Additional): H04L-009/32

File Segment: EPI

2/5/2 (Item 1 from file: 347)
DIALOG(R)File 347:JAPIO
(c) 2000 JPO & JAPIO. All rts. reserv.

05926923 **Image available**
AUTHENTICATION METHOD, CIPHER KEY SHARING METHOD, AND COMMUNICATION SYSTEM

PUB. NO.: 10-210023 A]
PUBLISHED: August 07, 1998 (19980807)
INVENTOR(s): SAI TAKAO

NAKAGAWA SATOSHI
NAKAI TOSHIHISA
TORII TAKASHI

APPLICANT(s): OKI ELECTRIC IND CO LTD [000029] (A Japanese Company or Corporation), JP (Japan)

APPL. NO.: 09-012876 [JP 9712876]

FILED: January 27, 1997 (19970127)
INTL CLASS: [6] H04L-009/08; H04L-009/32
JAPIO CLASS: 44.3 (COMMUNICATION -- Telegraphy); 44.2 (COMMUNICATION --
Transmission Systems)

ABSTRACT

PROBLEM TO BE SOLVED: To provide a new method which makes a second station authenticate a first station in a communication system including first and second stations which desire communication.

SOLUTION: Secret information $K(\text{sub } a)$ ($K'(\text{sub } a)$) common to a first station 11 and a second station 41 is stored in storage parts 13 and 43 of respective stations. The first station 11 transmits user information $I(\text{sub } a)$ identifying the first station to the second station 41. One of first and second stations generates random numbers (r) and transmits them to the other. The first station 11 uses random numbers, secret information, and a prescribed algorithm to generate first authentication information and transmits it to the second station 41. The second station 41 uses random numbers, secret information and a prescribed algorithm to generate second authentication information. The second station 41 compares first and second authentication information with each other and discriminates whether they coincide with each other or not to authenticate the validity of the first station.

【特許請求の範囲】

【請求項1】 共通の秘密情報をそれぞれの記憶手段に格納している第1の局および第2の局を含む通信システムにおいて、前記第2の局が前記第1の局を認証するに当たり、

前記第1の局が、第1の局である旨を示すユーザ情報を前記第2の局に送信する処理と、

前記第1および第2の局のいずれか一方が、乱数を発生しこれを他方の局に送信する処理と、

前記第1の局が、前記乱数と自局内の前記記憶手段に格納している前記秘密情報とを入力とする所定のアルゴリズムにより第1の認証情報を生成しこれを前記第2の局に送信する処理と、

前記第2の局が、前記乱数と自局内の前記記憶手段に格納している前記秘密情報とを入力とする所定のアルゴリズムにより第2の認証情報を生成する処理と、

前記第2の局が、前記第1の認証情報と前記第2の認証情報とを比較することにより前記第1の局の正当性を認証する処理とを含むことを特徴とする認証方法。

【請求項2】 共通の秘密情報をそれぞれの記憶手段に格納している第1の局および第2の局を含む通信システムにおいて、前記第2の局が前記第1の局を認証するに当たり、

前記第1の局が、第1の局である旨を示すユーザ情報を第2の局に送信する処理と、

前記第1の局が、乱数を発生する処理と、

前記第1の局が、該乱数を前記第2の局に送信する処理と、

前記第1の局が、前記乱数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより第1の認証情報を生成しこれを前記第2の局に送信する処理と、

前記第2の局が、前記送信されてきた乱数を認証する処理と、

前記乱数を認証する処理にて前記乱数が正当でないとされた場合に実行され、前記第2の局が前記第1の局を正当でないとする処理と、

前記乱数を認証する処理にて前記乱数が正当であるとされた場合に実行され、前記第2の局が、前記乱数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより第2の認証情報を生成し、かつ、前記第1の認証情報と前記第2の認証情報とを比較することにより前記第1の局の正当性を認証する処理とを含むことを特徴とする認証方法。

【請求項3】 共通の秘密情報をそれぞれの記憶手段に格納している第1の局および第2の局を含む通信システムにおいて、前記第2の局が前記第1の局を認証するに当たり、

前記第1の局が、第1の局である旨を示すユーザ情報を前記第2の局に送信する処理と、

10 前記第2の局が、前記送信されてきたアクセス回数を認証する処理と、

前記アクセス回数を認証する処理にて前記アクセス回数が正当でないとされた場合に実行され、前記第2の局が前記第1の局を正当でないとする処理と、

前記アクセス回数を認証する処理にて前記アクセス回数が正当であるとされた場合に実行され、前記第2の局が、前記乱数と前記アクセス回数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより第2の認証情報を生成し、かつ、前記第1の認証情報と前記第2の認証情報とを比較することにより前記第1の局の正当性を認証する処理とを含むことを特徴とする認証方法。

【請求項4】 共通の秘密情報をそれぞれの記憶手段に格納している第1の局および第2の局を含む通信システムにおいて、前記第2の局が前記第1の局を認証するに当たり、

前記第1の局が、第1の局である旨を示すユーザ情報を前記第2の局に送信する処理と、

前記第1の局が、乱数を発生する処理と、

30 前記第1の局が、自局内の前記記憶手段に格納してある前記秘密情報を鍵として前記乱数と前記ユーザ情報とを暗号化することにより認証情報を生成しこれを前記第2の局に送信する処理と、

前記第2の局が、自局内の前記記憶手段に格納してある前記秘密情報を鍵として前記送信されてきた認証情報を復号化する処理と、

前記第2の局が、前記復号化で得たユーザ情報と前記送信されてきたユーザ情報とを比較すること、および、前記復号化で得た乱数を認証することにより前記第1の局の正当性を認証する処理とを含むことを特徴とする認証方法。

【請求項5】 共通の秘密情報をそれぞれの記憶手段に格納している第1の局および第2の局を含む通信システムにおいて、前記第2の局が前記第1の局を認証するに当たり、

前記第1の局が、第1の局である旨を示すユーザ情報を前記第2の局に送信する処理と、

前記第1の局が第1の乱数および第2の乱数を発生する処理と、

50 前記第1の局が、第1の乱数を前記第2の局に送信する

処理と、

前記第1の局が、前記第2の乱数を鍵として前記ユーザ情報を暗号化して第1の暗号文を生成する処理と、

前記第1の局が、前記第1の乱数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより認証情報を生成するための暗号アルゴリズムの鍵を生成する処理と、

前記第1の局が、前記暗号アルゴリズムの鍵を用いて前記第2の乱数と前記第1の暗号文とをさらに暗号化して第2の暗号文を生成しこれを認証情報として前記第2の局に送信する処理と、

前記第2の局が、前記送信されてきた第1の乱数を認証する処理と、

前記第1の乱数を認証する処理にて前記第1の乱数が正当でないとされた場合に実行され、前記第2の局が前記第1の局を正当でないとする処理と、

前記第1の乱数を認証する処理にて前記第1の乱数が正当であるとされた場合に実行され、前記第2の局が、前記第1の乱数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより認証情報を復号化するための鍵を生成し、該鍵を用い前記送信されてきた認証情報を復号化し、該復号化で得たユーザ情報と前記送信されてきたユーザ情報とを比較することにより前記第1の局の正当性を認証する処理とを含むことを特徴とする認証方法。

【請求項6】 共通の秘密情報をそれぞれの記憶手段に格納している第1の局および第2の局を含む通信システムにおいて、前記第2の局が前記第1の局を認証するに当たり、

前記第1の局が、第1の局である旨を示すユーザ情報を前記第2の局に送信する処理と、

前記第1の局が、乱数を発生する処理と、

前記第1の局が、前記第2の局をアクセスした回数を計数する処理と、

前記第1の局が、前記乱数を鍵として前記ユーザ情報と前記アクセス回数とを暗号化する処理と、

前記第1の局が、自局内の前記記憶手段に格納してある前記秘密情報を鍵として前記暗号化されたユーザ情報と前記アクセス回数とをさらに暗号化してこれを認証情報として前記第2の局に送信する処理と、

前記第2の局が、自局内の前記記憶手段に記憶してある前記秘密情報を鍵として前記送信されてきた認証情報を復号化する処理と、

前記第2の局が、前記復号化で得たユーザ情報と前記送信されてきたユーザ情報とを比較すること、および、前記復号化で得たアクセス回数を認証することにより前記第1の局の正当性を認証する処理とを含むことを特徴とする認証方法。

【請求項7】 共通の秘密情報をそれぞれの記憶手段に格納している第1の局および第2の局を含む通信システ

ムにおいて、前記第2の局が前記第1の局を認証するに当たり、

前記第1の局が、第1の局である旨を示すユーザ情報を前記第2の局に送信する処理と、

前記第1の局が、第1の乱数および第2の乱数を発生する処理と、

前記第1の局が、該第1の乱数を前記第2の局に送信する処理と、

前記第1の局が、前記第2の局をアクセスした回数を計数する処理と、

前記第1の局が、前記第2の乱数を鍵として前記ユーザ情報と前記アクセス回数とを暗号化して第1の暗号文を生成する処理と、

前記第1の局が、前記第1の乱数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより認証情報を生成するための暗号アルゴリズムの鍵を生成する処理と、

前記第1の局が、前記暗号アルゴリズムの鍵を用いて前記第2の乱数と前記第1の暗号文とをさらに暗号化して第2の暗号文を生成しこれを認証情報として前記第2の局に送信する処理と、

前記第2の局が、前記第1の乱数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより前記認証情報を復号化するための鍵を生成する処理と、

前記第2の局が、前記復号化するための鍵を用い前記送信されてきた認証情報を復号化する処理と、

前記復号化で得たユーザ情報と前記送信されてきたユーザ情報とを比較すること、および、前記復号化で得たアクセス回数を認証することにより前記第1の局の正当性を認証する処理とを含むことを特徴とする認証方法。

【請求項8】 通信を希望する第1の局および第2の局と、該第2の局に代わって認証をする信頼できる第3の局とを含み、前記第1の局および第3の局は共通の秘密情報をそれぞれの記憶手段に格納している通信システムにおいて、前記第3の局が前記第1の局を認証するに当たり、

前記第1の局が、第1の局である旨を示すユーザ情報を前記第2の局に送信する処理と、

前記第1の局が、乱数を発生する処理と、

前記第1の局が、乱数を前記第2の局に送信する処理と、

前記第1の局が、前記乱数と自局内の前記記憶手段に格納してある前記秘密情報とを用いて認証情報を生成しこれを前記第2の局に送信する処理と、

前記第2の局が、前記第1の局から送信されてきたユーザ情報と乱数と認証情報とを前記第3の局に送信する処理と、

前記第3の局が、前記乱数と前記第2の局から送信されてきた認証情報を自局内の前記記憶手段に格納してある

10

20

30

40

50

前記秘密情報を用いて認証することにより前記第1の局の正当性を認証する処理と、

前記第3の局が、認証結果を前記第2の局に送信する処理とを含むことを特徴とする認証方法。

【請求項9】 通信を希望する第1の局および第2の局と、該第2の局に代わって認証をする信頼できる第3の局とを含み、前記第1の局および第3の局は共通の秘密情報をそれぞれの記憶手段に格納している通信システムにおいて、前記第3の局が前記第1の局を認証するに当たり、

前記第1の局が、第1の局である旨を示すユーザ情報を前記第2の局に送信する処理と、

前記第2の局が、前記ユーザ情報を受信すると乱数を発生し該乱数を前記第1の局に送信する処理と、

前記第1の局が、前記第2の局から送信されてきた乱数と自局内の前記記憶手段に格納している前記秘密情報とを用いて認証情報を生成しこれを前記第2の局に送信する処理と、

前記第2の局が、前記乱数と前記第1の局から送信されてきたユーザ情報と認証情報とを前記第3の局に送信する処理と、

前記第3の局が、前記第2の局から送信されてきた認証情報を自局内の前記記憶手段に格納してある前記秘密情報を用いて認証することにより前記第1の局の正当性を認証する処理と前記第3の局が、認証結果を前記第2の局に送信する処理とを含むことを特徴とする認証方法。

【請求項10】 通信を希望する第1の局および第2の局と、これら局間に介在する中間局とを含み、前記第1の局および第2の局は共通の秘密情報をそれぞれの記憶手段に格納している通信システムにおいて、前記第2の局が前記第1の局を認証するに当たり、

前記第1の局が、第1の局である旨を示すユーザ情報を前記中間局に送信する処理と、

前記中間局が、前記ユーザ情報を受信すると乱数を発生し該乱数を前記第1の局に送信する処理と、

前記第1の局が、前記中間局から送信されてきた乱数と自局内の前記記憶手段に格納している前記秘密情報とを用いて認証情報を生成しこれを前記中間局に送信する処理と、

前記中間局が、前記乱数と前記第1の局から送信されてきたユーザ情報と認証情報とを前記第2の局に送信する処理と、

前記第2の局が、前記中間局から送信されてきた認証情報を自局内の前記記憶手段に格納している前記秘密情報を用いて認証することにより前記第1の局の正当性を認証する処理とを含むことを特徴とする認証方法。

【請求項11】 請求項1～3のいずれか1項に記載の認証方法において、

前記第1の局および第2の局それぞれに、前記所定のアルゴリズムとして用いることができるアルゴリズムを複

数種かつ同様に予め用意しておく、

前記第1または第2の局が選択信号を発生しこれに応じ前記第1および第2の局それぞれが前記複数種のアルゴリズムの中から1つを選択し、

該選択されたアルゴリズムにより前記第1の局は前記第1の認証情報を生成し、前記第2の局は前記第2の認証情報を生成することを特徴とする認証方法。

【請求項12】 請求項2に記載の認証方法において、前記送信されてきた乱数を認証する処理とは、

10 前記第1の局から送信されてくる乱数の履歴を記憶し、かつ、今回の通信で前記第1の局から送信されてきた乱数が前回の通信までの乱数履歴中に含まれているか否かを調べる処理であることを特徴とする認証方法。

【請求項13】 請求項4に記載の認証方法において、前記復号化で得た乱数を認証する処理とは、

復号化で得られる乱数の履歴を記憶し、かつ、今回の通信での復号化で得られた乱数が前回の通信までの乱数履歴中に含まれているか否かを調べる処理であることを特徴とする認証方法。

20 【請求項14】 請求項5に記載の認証方法において、前記送信されてきた第1の乱数を認証する処理とは、前記第1の局から送信されてくる第1の乱数の履歴を記憶し、かつ、今回の通信で前記第1の局から送信された第1の乱数が前回の通信までの乱数履歴中に含まれているか否かを調べる処理であることを特徴とする認証方法。

【請求項15】 請求項3に記載の認証方法において、前記送信されてきたアクセス回数を認証する処理とは、前記第1の局から送信される前記アクセス回数を記憶し、かつ、今回の通信で前記第1の局から送信されたアクセス回数が前回の通信までのアクセス回数に対し所定の不等式関係を満たすか否かを調べる処理であることを特徴とする認証方法。

【請求項16】 請求項6または7に記載の認証方法において、

前記復号化で得たアクセス回数を認証する処理とは、前記第2の局が復号化で得たアクセス回数を記憶し、かつ、今回の通信での復号化で得たアクセス回数が前回の通信での復号化で得たアクセス回数に対し所定の不等式関係を満たすか否かを調べる処理であることを特徴とする認証方法。

【請求項17】 請求項5または7に記載の認証方法において、

前記第1の局および第2の局それぞれに、前記所定のアルゴリズムとして用いることができるアルゴリズムを複数種かつ同様に予め用意しておく、

前記第1または第2の局が選択信号を発生しこれに応じ前記第1および第2の局それぞれが前記複数種のアルゴリズムの中から1つを選択し、

50 該選択されたアルゴリズムにより、前記第1の局は前記

暗号アルゴリズムの鍵を生成し、前記第2の局は前記認証情報を復号化するための鍵を生成することを特徴とする認証方法。

【請求項18】 請求項1、2、3、5、7、11または17に記載の認証方法において、前記所定のアルゴリズムを一方向性関数とすることを特徴とする認証方法。

【請求項19】 請求項4～7のいずれか1項に記載の認証方法において、

前記第1の局および第2の局それぞれに、前記認証情報を生成する際のアルゴリズムおよび前記認証情報を復号化する際のアルゴリズムとして用いることができる複数種の暗号アルゴリズムを同様に予め用意しておき、

前記第1または第2の局が選択信号を発生しこれに応じ前記第1および第2の局それぞれが前記複数種の暗号アルゴリズムの中から1つを選択し、

該選択された暗号アルゴリズムにより、前記第1の局は前記認証情報を生成する暗号化をし、前記第2の局は前記認証情報を復号化することを特徴とする認証方法。

【請求項20】 請求項1～3のいずれか1項に記載の認証方法により前記第1の局について認証をし、

該認証により正当とされた場合は前記第1の局および第2の局それぞれで前記乱数および前記秘密情報を入力とする所定の暗号鍵生成アルゴリズムにより共有暗号鍵をそれぞれ生成し、

これを前記第1および第2の局の共有暗号鍵とすることを特徴とする暗号鍵共有方法。

【請求項21】 請求項4または6に記載の認証方法により前記第1の局について認証をし、

該認証により正当とされた場合は前記第1の局および第2の局それぞれで前記乱数を入力とする所定の暗号鍵生成アルゴリズムにより共有暗号鍵をそれぞれ生成し、

これを前記第1および第2の局の共有暗号鍵とすることを特徴とする暗号鍵共有方法。

【請求項22】 請求項5または7に記載の認証方法により前記第1の局について認証をし、

該認証により正当とされた場合は前記第1の局および第2の局それぞれで前記第2の乱数を入力とする所定の暗号鍵生成アルゴリズムにより共有暗号鍵をそれぞれ生成し、

これを前記第1および第2の局の共有暗号鍵とすることを特徴とする暗号鍵共有方法。

【請求項23】 請求項20～22のいずれか1項に記載の暗号鍵共有方法において、

前記第1の局および第2の局それぞれに、前記所定の暗号鍵生成アルゴリズムとして用いることができるアルゴリズムを複数種かつ同様に予め用意しておき、

前記第1または第2の局が選択信号を発生しこれに応じ前記第1および第2の局それぞれが前記複数種の暗号鍵生成アルゴリズムの中から1つを選択し、

該選択された暗号鍵生成アルゴリズムにより、前記第1の局および第2の局は共有暗号鍵をそれぞれ生成することを特徴とする暗号鍵共有方法。

【請求項24】 請求項8または9に記載の認証方法により前記第1の局について認証をし、

該認証により正当とされた場合は前記第1の局および第3の局それぞれで共有暗号鍵をそれぞれ生成し、

前記第3の局は該共有暗号鍵を前記第2の局に送信しこれを前記第2の局は共有暗号鍵とすることを特徴とする暗号鍵共有方法。

【請求項25】 請求項10に記載の認証方法により前記第1の局について認証をし、

該認証において正当とされた場合は、前記第1の局および第2の局それぞれで共有暗号鍵をそれぞれ生成し、これを前記第1および第2の局の共有暗号鍵とすることを特徴とする暗号鍵共有方法。

【請求項26】 共通の秘密情報をそれぞれの記憶手段に格納している第1の局および第2の局を含む通信システムにおいて、

(1) 前記第1の局から前記第2の局に第1の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段と、

(2) 前記第1の局または前記第2の局に設けられ、乱数を発生するための乱数生成手段と、

(3) 前記発生された乱数を他方の局に送信するための乱数送信手段と、

(4) 前記第1の局に設けられ、前記乱数と自局内の前記記憶手段に格納された前記秘密情報とを入力とする所定のアルゴリズムにより第1の認証情報を生成するための第1の認証情報生成手段と、

(5) 前記第1の認証情報を前記第2の局に送信するための認証情報送信手段と、

(6) 前記第2の局に設けられ、前記乱数と自局内の前記記憶手段に格納された前記秘密情報とを入力とする所定のアルゴリズムにより第2の認証情報を生成するための第2の認証情報生成手段と、

(7) 前記第2の局に設けられ、前記第1の認証情報と前記第2の認証情報とを比較することで前記第1の局の正当性を認証するための認証手段とを具備したことを特徴とする通信システム。

【請求項27】 共通の秘密情報をそれぞれの記憶手段に格納している第1の局および第2の局を含む通信システムにおいて、

(1) 前記第1の局から前記第2の局に第1の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段と、

(2) 前記第1の局に設けられ、乱数を発生するための乱数生成手段と、

(3) 前記発生された乱数を前記第2の局に送信するための乱数送信手段と、

(4) 前記第1の局に設けられ、前記乱数と自局内の前記記憶手段に格納された前記秘密情報とを入力とする所定のアルゴリズムにより第1の認証情報を生成するための第1の認証情報生成手段と、

(5) 前記第1の認証情報を前記第2の局に送信するための認証情報送信手段と、

(6) 前記第2の局に設けられ、前記送信されてくる乱数を認証するための乱数認証手段と、

(7) 前記第2の局に設けられ、前記送信されてくる乱数と自局内の前記記憶手段に格納された前記秘密情報とを入力とする所定のアルゴリズムにより第2の認証情報を生成するための第2の認証情報生成手段と、

(8) 前記第2の局に設けられ、前記第1の認証情報と前記第2の認証情報とを比較することにより前記第1の局の正当性を認証するための認証手段とを具えたことを特徴とする通信システム。

【請求項28】 共通の秘密情報をそれぞれの記憶手段に格納している第1の局および第2の局を含む通信システムにおいて、

(1) 前記第1の局から前記第2の局に第1の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段と、

(2) 前記第1の局または前記第2の局に設けられ、乱数を発生するための乱数生成手段と、

(3) 前記発生された乱数を他方の局に送信するための乱数送信手段と、

(4) 前記第1の局に設けられ、前記第1の局が前記第2の局をアクセスしたアクセス回数を計数するためのアクセス回数計数手段と、

(5) 前記アクセス回数を前記第2の局に送信するためのアクセス回数送信手段と、

(6) 前記第1の局に設けられ、前記アクセス回数と前記乱数と自局内の前記記憶手段に格納された前記秘密情報とを入力とする所定のアルゴリズムにより第1の認証情報を生成するための第1の認証情報生成手段と、

(7) 前記第1の認証情報を前記第2の局に送信するための認証情報送信手段と、

(8) 前記第2の局に設けられ、前記送信されてくるアクセス回数を認証するためのアクセス回数認証手段と、

(9) 前記第2の局に設けられ、前記送信されてくるアクセス回数と前記乱数と自局内の前記記憶手段に格納された前記秘密情報とを入力とする所定のアルゴリズムにより第2の認証情報を生成するための第2の認証情報生成手段と、

(10) 前記第2の局に設けられ、前記第1の認証情報と前記第2の認証情報とを比較することで前記第1の局の正当性を認証するための認証手段とを具えたことを特徴とする通信システム。

【請求項29】 共通の秘密情報をそれぞれの記憶手段に格納している第1の局および第2の局を含む通信シ

テムにおいて、

(1) 前記第1の局から前記第2の局に第1の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段と、

(2) 前記第1の局に設けられ、乱数を発生するための乱数生成手段と、

(3) 前記第1の局に設けられ、自局内の前記記憶手段に格納してある前記秘密情報を鍵として前記乱数と前記ユーザ情報とを暗号化することにより認証情報を生成するための認証情報生成手段と、

(4) 前記認証情報を前記第2の局に送信するための認証情報送信手段と、

(5) 前記第2の局に設けられ、自局内の前記記憶手段に格納してある前記秘密情報を鍵として前記送信されてくる認証情報を復号化するための認証情報復号化手段と、

(6) 前記第2の局に設けられ、前記復号化により得られたユーザ情報と前記送信されてくるユーザ情報とを比較すること、および、前記復号化により得られた乱数を認証することにより前記第1の局の正当性を認証するための認証手段とを具えたことを特徴とする通信システム。

【請求項30】 共通の秘密情報をそれぞれの記憶手段に格納している第1の局および第2の局を含む通信システムにおいて、

(1) 前記第1の局から前記第2の局に対し第1の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段と、

(2) 前記第1の局に設けられ、第1の乱数および第2の乱数を発生するための乱数生成手段と、

(3) 前記発生された第1の乱数を前記第2の局に送信するための乱数送信手段と、

(4) 前記第1の局に設けられ、前記第2の乱数を鍵として前記ユーザ情報を暗号化して第1の暗号文を生成するための暗号文生成手段と、

(5) 前記第1の局に設けられ、前記第1の乱数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより認証情報を生成するための暗号アルゴリズムの鍵を生成するための暗号鍵生成手段と、

(6) 前記第1の局に設けられ、前記暗号アルゴリズムの鍵を用いて前記第2の乱数と前記第1の暗号文とをさらに暗号化して認証情報としての第2の暗号文を生成するための認証情報生成手段と、

(7) 前記認証情報を前記第2の局に送信するための認証情報送信手段と、

(8) 前記第2の局に設けられ、前記送信されてくる第1の乱数を認証するための乱数認証手段と、

(9) 前記第2の局に設けられ、前記送信されてくる第1の乱数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより前記認証情報を復号化するための鍵を生成するための復号鍵生成

10

20

30

40

50

手段と、

(10) 前記第2の局に設けられ、前記復号鍵を用いて前記認証情報を復号化するための認証情報復号化手段と、

(11) 前記第2の局に設けられ、前記復号化により得られたユーザ情報と前記送信されてくるユーザ情報とを比較することにより前記第1の局の正当性を認証するための認証手段とを具えたことを特徴とする通信システム。

【請求項31】 共通の秘密情報をそれぞれの記憶手段に格納している第1の局および第2の局を含む通信システムにおいて、

(1) 前記第1の局から前記第2の局に対し第1の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段と、

(2) 前記第1の局に設けられ、乱数を発生するための乱数生成手段と、

(3) 前記第1の局に設けられ、前記第1の局が前記第2の局をアクセスしたアクセス回数を計数するためのアクセス回数計数手段と、

(4) 前記第1の局に設けられ、前記乱数を鍵として前記ユーザ情報と前記アクセス回数とを暗号化するための暗号化手段と、

(5) 前記第1の局に設けられ、自局内の前記記憶手段に格納してある前記秘密情報を鍵として前記暗号化されたユーザ情報とアクセス回数とをさらに暗号化することにより認証情報を生成するための認証情報生成手段と、

(6) 前記認証情報を前記第2の局に送信するための認証情報送信手段と、

(7) 前記第2の局に設けられ、自局内の前記記憶手段に格納してある前記秘密情報を鍵として前記送信されてくる認証情報を復号化するための認証情報復号化手段と、

(8) 前記第2の局に設けられ、前記復号化により得られるユーザ情報と前記送信されてくるユーザ情報とを比較すること、および、前記復号化により得られるアクセス回数を認証することにより前記第1の局の正当性を認証するための認証手段とを具えたことを特徴とする通信システム。

【請求項32】 共通の秘密情報をそれぞれの記憶手段に格納している第1の局および第2の局を含む通信システムにおいて、

(1) 前記第1の局から前記第2の局に対し第1の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段と、

(2) 前記第1の局に設けられ、第1の乱数および第2の乱数を発生するための乱数生成手段と、

(3) 前記発生された第1の乱数を前記第2の局に送信するための乱数送信手段と、

(4) 前記第1の局に設けられ、前記第1の局が前記第2の局をアクセスしたアクセス回数を計数するためのアクセス回数計数手段と、

(5) 前記第1の局に設けられ、前記第2の乱数を鍵とし

て前記ユーザ情報と前記アクセス回数とを暗号化して第1の暗号文を生成するための暗号文生成手段と、

(6) 前記第1の局に設けられ、前記第1の乱数と自局内の前記記憶手段に格納してある前記秘密情報とを人力とする所定のアルゴリズムにより認証情報を生成するための暗号アルゴリズムの鍵を生成するための暗号鍵生成手段と、

(7) 前記第1の局に設けられ、前記暗号アルゴリズムの鍵を用いて前記第2の乱数と前記第1の暗号文とをさらに暗号化して認証情報としての第2の暗号文を生成するための認証情報生成手段と、

(8) 前記認証情報を前記第2の局に送信するための認証情報送信手段と、

(9) 前記第2の局に設けられ、前記送信されてくる第1の乱数と自局内の前記記憶手段に格納してある前記秘密情報とを人力とする所定のアルゴリズムにより前記認証情報を復号化するための鍵を生成するための復号鍵生成手段と、

(10) 前記第2の局に設けられ、前記送信されてくる認証情報を前記復号鍵を用い復号化するための認証情報復号化手段と、

(11) 前記第2の局に設けられ、前記復号化により得られるユーザ情報と前記送信されてくるユーザ情報とを比較すること、および、前記復号化により得られるアクセス回数を認証することにより前記第1の局の正当性を認証するための認証手段とを具えたことを特徴とする通信システム。

【請求項33】 通信を希望する第1の局および第2の局と、該第2の局に代わって認証をする信頼できる第3の局とを含み、前記第1の局および第3の局は共通の秘密情報をそれぞれの記憶手段に格納している通信システムにおいて、

(1) 前記第1の局から前記第2の局に第1の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段と、

(2) 前記第1の局に設けられ、乱数を発生するための乱数生成手段と、

(3) 前記発生された乱数を前記第2の局に送信するための乱数送信手段と、

(4) 前記第1の局に設けられ、前記乱数と自局内の前記記憶手段に格納された前記秘密情報とを用い認証情報を生成するための認証情報生成手段と、

(5) 前記認証情報を前記第2の局に送信するための認証情報送信手段と、

(6) 前記第1の局から前記第2の局に送信されてくる前記ユーザ情報、前記乱数および前記認証情報それぞれを前記第3の局に送信するための送信手段と、

(7) 前記第3の局に設けられ、前記第2の局から送信されてくる前記認証情報を自局内の前記記憶手段に格納してある前記秘密情報をを用いて認証することにより前記第

1の局の正当性を認証するための認証手段と、

(8) 前記第3の局に設けられ、前記認証結果を前記第2の局に送信するための認証結果送信手段とを具えたことを特徴とする通信システム、

【請求項34】 通信を希望する第1の局および第2の局と、該第2の局に代わって認証をする信頼できる第3の局とを含み、前記第1の局および第3の局は共通の秘密情報をそれぞれの記憶手段に格納している通信システムにおいて、

(1) 前記第1の局から前記第2の局に第1の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段と、

(2) 前記第2の局に設けられ、前記ユーザ情報を受信すると乱数を発生するための乱数生成手段と、

(3) 前記発生された乱数を前記第1の局に送信するための乱数送信手段と、

(4) 前記第1の局に設けられ、前記乱数と自局内の前記記憶手段に格納された前記秘密情報とを用い認証情報を生成するための認証情報生成手段と、

(5) 前記認証情報を前記第2の局に送信するための認証情報送信手段と、

(6) 前記乱数と前記第1の局から前記第2の局に送信されてくる前記ユーザ情報および前記認証情報を前記第3の局に送信するための送信手段と、

(7) 前記第3の局に設けられ、前記第2の局から送信されてくる前記認証情報を自局内の前記記憶手段に格納してある前記秘密情報を用いて認証することにより前記第1の局の正当性を認証するための認証手段と、

(8) 前記第3の局に設けられ、前記認証結果を前記第2の局に送信するための認証結果送信手段とを具えたことを特徴とする通信システム。

【請求項35】 通信を希望する第1の局および第2の局と、これら局間に介在する中間局とを含み、前記第1の局および第2の局は共通の秘密情報をそれぞれの記憶手段に格納している通信システムにおいて、

(1) 前記第1の局から前記中間局に第1の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段と、

(2) 前記中間局に設けられ、前記ユーザ情報を受信すると乱数を発生するための乱数生成手段と、

(3) 前記発生された乱数を前記第1の局に送信するための乱数送信手段と、

(4) 前記第1の局に設けられ、前記送信されてくる乱数と自局内の前記記憶手段に格納してある前記秘密情報とを用いて認証情報を生成するための認証情報生成手段と、

(5) 前記認証情報を前記中間局に送信するための認証情報送信手段と、

(6) 前記乱数と第1の局から前記中間局に送信されてくる前記ユーザ情報および前記認証情報を前記第2の局に

送信するための送信手段と、

(7) 前記第2の局に設けられ、前記送信されてくる認証情報を自局内の前記記憶手段に格納してある前記秘密情報を用い認証することにより前記第1の局の正当性を認証するための認証手段とを具えたことを特徴とする通信システム。

【請求項36】 請求項26～28のいずれか1項に記載の通信システムにおいて、

前記第1の局および第2の局それぞれに設けられかつ前記所定のアルゴリズムとして使用できるアルゴリズムを複数格納している記憶手段と、

前記第1の局および第2の局のいずれか一方でアルゴリズム選択信号を発生しこれを他方の局にも送信し、しかも、これら選択信号により前記第1の局および第2の局それぞれの前記複数のアルゴリズムを記憶している記憶手段から共通の1つのアルゴリズムをそれぞれ選択してこれをそれぞれの局に備わる前記第1または第2の認証情報生成手段に前記所定のアルゴリズムとして出力するアルゴリズム選択手段とを具えたことを特徴とする通信システム。

【請求項37】 請求項27に記載の通信システムにおいて、

前記乱数認証手段として、

前記第2の局に設けられ前記第1の局から送信されてくる乱数の履歴を記憶するための手段と、

前記第2の局に設けられ今回の通信で前記第1の局から送信されてくる乱数が前回の通信までの乱数履歴に含まれているか否かを調べるための比較手段とを含むことを特徴とする通信システム。

【請求項38】 請求項29に記載の通信システムにおいて、

前記復号化により得られた乱数を認証する手段として、前記第2の局に設けられ、復号化で得られる乱数の履歴を記憶するための手段と、

前記第2の局に設けられ今回の通信での復号化で得られた乱数が前回の通信までの乱数履歴に含まれているか否かを調べるための比較手段とを含むことを特徴とする通信システム。

【請求項39】 請求項30に記載の通信システムにおいて、

前記第1の乱数を認証するための手段として、

前記第2の局に設けられ前記第1の局から送信されてくる第1の乱数の履歴を記憶するための手段と、

前記第2の局に設けられ今回の通信で前記第1の局から送信されてくる第1の乱数が前回の通信までの乱数履歴に含まれているか否かを調べるための比較手段とを含むことを特徴とする通信システム。

【請求項40】 請求項28に記載の通信システムにおいて、

前記アクセス回数認証手段として、

前記第 2 の局に設けられ、前記第 1 の局から送信されてくるアクセス回数を記憶するための手段と、

前記第 2 の局に設けられ今回の通信で前記第 1 の局から送信されてくるアクセス回数が前回の通信までのアクセス回数に対し所定の不等式関係を満たすか否かを調べるための比較手段とを含むことを特徴とする通信システム。

【請求項 4 1】 請求項 3 1 または 3 2 に記載の通信システムにおいて、

前記復号化で得られたアクセス回数を認証するための手段として、

前記第 2 の局に設けられ、復号化で得られるアクセス回数を記憶する手段と、

前記第 2 の局に設けられ今回の通信での復号化で得られた乱数が前回の通信での復号化で得られたアクセス回数に対し所定の不等式関係を満たすか否かを調べるための比較手段とを含むことを特徴とする通信システム。

【請求項 4 2】 請求項 3 0 または 3 2 に記載の通信システムにおいて、

前記第 1 の局および第 2 の局それぞれに設けられかつ前記所定のアルゴリズムとして使用できるアルゴリズムを複数格納している記憶手段と、

前記第 1 の局および第 2 の局のいずれか一方でアルゴリズム選択信号を発生しこれを他方の局にも送信し、しかも、これら選択信号により前記第 1 の局および第 2 の局それぞれの前記複数のアルゴリズムを記憶している記憶手段から共通の 1 つのアルゴリズムをそれぞれ選択してこれをそれぞれの局に備わる前記暗号鍵生成手段または復号鍵生成手段に前記所定のアルゴリズムとして出力するアルゴリズム選択手段とを具えたことを特徴とする通信システム。

【請求項 4 3】 請求項 2 6、2 7、2 8、3 0、3 2、3 6 または 4 2 に記載の通信システムにおいて、前記所定のアルゴリズムを一方方向性関数とすることを特徴とする通信システム。

【請求項 4 4】 請求項 2 7 に記載の通信システムにおいて、

前記乱数認証手段は、前記乱数が正当でないと判断した場合、前記第 1 の局を正当でないと決定し、

前記第 2 の認証情報生成手段および前記認証手段それぞれを、前記乱数認証手段が前記乱数を正当と判断した場合に動作する手段とすることを特徴とする通信システム。

【請求項 4 5】 請求項 2 8 に記載の通信システムにおいて、

前記アクセス回数認証手段は、前記アクセス回数が正当でないと判断した場合、前記第 1 の局を正当でないと決定し、

前記第 2 の認証情報生成手段および前記認証手段それぞれを、前記アクセス回数認証手段が前記アクセス回数を

正当と判断した場合に動作する手段とすることを特徴とする通信システム。

【請求項 4 6】 請求項 3 0 に記載の通信システムにおいて、

前記第 1 の乱数認証手段は、前記第 1 の乱数が正当でないと判断した場合、前記第 1 の局を正当でないと決定し、

前記復号鍵生成手段、前記認証情報復号化手段および前記認証手段それぞれを、前記第 1 の乱数認証手段が前記第 1 の乱数を正当と判断した場合に動作する手段とすることを特徴とする通信システム。

【請求項 4 7】 請求項 2 9～3 2 のいずれか 1 項に記載の通信システムにおいて、

前記第 1 の局および第 2 の局それぞれに設けられかつ前記認証情報生成手段および前記認証情報復号化手段で使用する暗号アルゴリズムを複数格納している記憶手段と、

前記第 1 の局および第 2 の局のいずれか一方でアルゴリズム選択信号を発生しこれを他方の局にも送信し、しかも、これら選択信号により前記第 1 の局および第 2 の局それぞれの前記複数の暗号アルゴリズムを記憶している記憶手段から共通の 1 つのアルゴリズムをそれぞれ選択してこれをそれぞれの局に備わる前記認証情報生成手段または認証情報復号化手段に出力するアルゴリズム選択手段とを具えたことを特徴とする通信システム。

【請求項 4 8】 請求項 2 6～2 8 のいずれか 1 項に記載の通信システムにおいて、

前記第 1 の局および第 2 の局それぞれに設けられ、前記認証手段により前記第 1 の局が正当であるとされた場合に動作し、前記乱数および前記秘密情報を入力とする暗号鍵生成アルゴリズムにより共有暗号鍵を生成する共有暗号鍵生成手段をさらに具えたことを特徴とする通信システム。

【請求項 4 9】 請求項 2 9 または 3 1 に記載の通信システムにおいて、

前記第 1 の局および第 2 の局それぞれに設けられ、前記認証手段により前記第 1 の局が正当であるとされた場合に動作し、前記乱数を入力とする暗号鍵生成アルゴリズムにより共有暗号鍵を生成する共有暗号鍵生成手段をさらに具えたことを特徴とする通信システム。

【請求項 5 0】 請求項 3 0 または 3 2 に記載の通信システムにおいて、

前記第 1 の局および第 2 の局それぞれに設けられ、前記認証手段により前記第 1 の局が正当であるとされた場合に動作し、前記第 2 の乱数を入力とする暗号鍵生成アルゴリズムにより共有暗号鍵を生成する共有暗号鍵生成手段をさらに具えたことを特徴とする通信システム。

【請求項 5 1】 請求項 4 8～5 0 のいずれか 1 項に記載の通信システムにおいて、

前記第 1 の局および第 2 の局それぞれに設けられ、前記

暗号鍵生成アルゴリズムとして用いることができるアルゴリズムを複数格納している記憶手段と、前記第1の局および第2の局のいずれか一方でアルゴリズム選択信号を発生しこれを他方の局にも送信し、しかも、これら選択信号により前記第1の局および第2の局それぞれの前記複数の暗号アルゴリズムを記憶している記憶手段から共通の1つのアルゴリズムをそれぞれ選択してこれをそれぞれの局に備わる共有暗号鍵生成手段に出力する、アルゴリズム選択手段とを具えたことを特徴とする通信システム。

【請求項52】 請求項33または34に記載の通信システムにおいて、

前記第1の局および第3の局それぞれに設けられ、前記認証手段により前記第1の局が正当であるとされた場合に動作する共有暗号鍵生成手段と、

前記第3の局で生成された共有暗号鍵を前記第2の局に送信するための共有暗号鍵送信手段とを具えたことを特徴とする通信システム。

【請求項53】 請求項35に記載の通信システムにおいて、

前記第1の局および第2の局それぞれに設けられ、前記認証手段により前記第1の局が正当であるとされた場合に動作する共有暗号鍵生成手段を具えたことを特徴とする通信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、通信を行う一対の通信者の間で通信相手を認証する方法と、暗号通信を行なう際の共有暗号鍵（暗号化用の鍵と復号化用の鍵が同一な暗号鍵）の作成方法と、その実施に好適な通信システムとに関するものである。

【0002】

【従来の技術】暗号通信を行うとき、共有暗号鍵を通信者間でどのように共有するかが重要な問題の一つになる。例えば文献I（IEEE Trans.on Inform.Theory(アイーイー トランザクション オン インフォーマション セリ), IT-22, No. 6, pp. 644-654(1976)）および文献Iを引用した文献II（「暗号と情報セキュリティ」、辻井 重男、笠原 正雄 編著、昭晃堂、pp. 72-73、(1990)）には、事前に秘密情報を共有せずに共有暗号鍵を生成する方法が開示されている。具体的には、通信者A、Bが暗号鍵を交換したいと仮定する。大きい素数 n （512ビット程度）と、 n 個の要素を持つ有限体 $GF(n)$ の原始元である整数 g とを公開して、次のように通信者A、Bの共有暗号鍵を生成している。

【0003】（1）Aは乱数 x を生成し、そして $X = g^{x \bmod n}$ をBに送信する。なお、 $g^{x \bmod n}$ とは g^x を n で割った余りを表す（以下の $g^y \bmod n$ などにおいて同様。）。

【0004】（2）Bは乱数 y を生成し、そして $Y = g^{y \bmod n}$ をAに送信する。

$Y \bmod n$ をAに送信する。

【0005】（3）Aは $K_A = Y^x \bmod n$ のように暗号鍵を生成する。

【0006】（4）Bは $K_B = X^y \bmod n$ のように暗号鍵を生成する。

【0007】簡単な演算により、 $K_A = K_B = g^{xy \bmod n}$ を得ることができる。この値を通信者A、Bの共有暗号鍵とする。一方、第3者がこの暗号鍵を解読する場合、これが離散対数問題であるため現実的な時間で解を求めることが難しい。したがって、通信者A、B間での暗号鍵の共有を確保することができる。

【0008】

【発明が解決しようとする課題】しかしながら上述した従来の方法では、通信相手を認証する方法が示されていない。

【0009】そのため、通信相手の認証がなされないまま暗号鍵を生成することになる。したがって、例えば通信中に通信情報が第3者（正当でない通信者）に盗聴されて改竄されても、改竄された情報により暗号鍵が計算されてしまうので、暗号鍵を共有することができなくなる場合もある。

【0010】したがって通信相手を認証するための新規な方法が望まれる。

【0011】また、通信相手を認証するための新規な方法が開発されても、その新規な認証方法で認証作業が終了後に別途に通信者間で暗号鍵共有のための情報通信を行なうのでは、その通信作業中にやはり第3者による盗聴や攻撃がなされてしまう危険がある。

【0012】したがって通信相手を認証することと併せて通信者間の暗号鍵の共有も行なうことができる暗号鍵共有方法の実現が望まれる。

【0013】また、上記の認証方法や暗号鍵共有方法の実施に好適な通信システムの実現が望まれる。

【0014】

【課題を解決するための手段】

（1）そこでこの出願の認証方法の第1の発明によれば、共通の秘密情報をそれぞれの記憶手段に格納している第1の局および第2の局を含む通信システムにおいて、前記第2の局が前記第1の局を認証するに当たり、以下の各処理を含むことを特徴とする。

【0015】(a) 前記第1の局が、第1の局である旨を示すユーザ情報を前記第2の局に送信する処理。(b) 前記第1の局または第2の局が、乱数を発生してこれを他方の局に送信する処理。(c) 前記第1の局が、前記乱数と自局内の前記記憶手段に格納している前記秘密情報とを入力とする所定のアルゴリズムにより第1の認証情報を生成しこれを前記第2の局に送信する処理。(d) 前記第2の局が、前記乱数と自局内の前記記憶手段に格納している前記秘密情報とを入力とする所定のアルゴリズムにより第2の認証情報を生成する処理。(e) 前記第2の

局が、前記第 1 の認証情報と前記第 2 の認証情報とを比較することにより前記第 1 の局の正当性を認証する処理。

【0016】ここで秘密情報は、第 1 の局と第 2 の局とで共有することができる予め定めた任意の秘密の情報である（以下の各発明において同じ。）。またユーザ情報は、第 1 の局に固有の任意の情報であり、例えばユーザ ID や名前（人名などに限らない任意のもの）やメールアドレスなどである（以下の各発明において同じ。）。

【0017】この認証方法の第 1 の発明によれば、第 1 の局が第 2 の局にユーザ情報を送信すると認証動作が開始される。また認証は、第 1 の局および第 2 の局に共通な秘密情報、乱数および所定のアルゴリズムを用い各局が生成する第 1 および第 2 の認証情報の一致・不一致を判定することで、なされる。

【0018】この認証方法の第 1 の発明を実施するため、以下の(1)～(7)の手段を具えた通信システム（通信システムの第 1 の発明）を構成するのが好適である。

【0019】(1) 前記第 1 の局から前記第 2 の局に第 1 の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段。(2) 前記第 1 の局または前記第 2 の局に設けられ、乱数を発生するための乱数生成手段。(3) 前記発生された乱数を他方の局に送信するための乱数送信手段。(4) 前記第 1 の局に設けられ、前記乱数と自局内の前記記憶手段に格納された前記秘密情報とを入力とする所定のアルゴリズムにより第 1 の認証情報を生成するための第 1 の認証情報生成手段。(5) 前記第 1 の認証情報を前記第 2 の局に送信するための認証情報送信手段。(6) 前記第 2 の局に設けられ、前記乱数と自局内の前記記憶手段に格納された前記秘密情報とを入力とする所定のアルゴリズムにより第 2 の認証情報を生成するための第 2 の認証情報生成手段。(7) 前記第 2 の局に設けられ、前記第 1 の認証情報と前記第 2 の認証情報とを比較することで前記第 1 の局の正当性を認証するための認証手段。

【0020】(2) また、この出願の認証方法の第 2 の発明によれば、共通の秘密情報をそれぞれの記憶手段に格納している第 1 の局および第 2 の局を含む通信システムにおいて、前記第 2 の局が前記第 1 の局を認証するに当たり、以下の各処理を含むことを特徴とする。

【0021】(a) 前記第 1 の局が、第 1 の局である旨を示すユーザ情報を前記第 2 の局に送信する処理。(b) 前記第 1 の局が、乱数を発生する処理。(c) 第 1 の局が、前記乱数を第 2 の局に送信する処理。(d) 前記第 1 の局が、前記乱数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより第 1 の認証情報を生成しこれを前記第 2 の局に送信する処理。(e) 前記第 2 の局が、前記送信されてきた乱数を認証する処理。(f) 前記乱数を認証する処理にて前記乱数が正当でないとされた場合に実行され、前記第 2 の局が

前記第 1 の局を正当でないとする処理。(g) 前記乱数を認証する処理にて前記乱数が正当であるとされた場合に実行され、前記第 2 の局が、前記乱数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより第 2 の認証情報を生成し、かつ、前記第 1 の認証情報と前記第 2 の認証情報とを比較することにより前記第 1 の局の正当性を認証する処理。

【0022】この認証方法の第 2 の発明によれば、第 1 の局が第 2 の局にユーザ情報および乱数を送信すると認証動作が開始される。また認証は、第 1 の局から送信されてきた乱数に対し先ず行なうことができる。乱数の認証は、例えば、第 1 の局から今回送信されてきた乱数が第 1 の局から過去に送られた乱数履歴に含まれているか否かを調べることにより行なうことができる。

【0023】乱数の認証は次の様な役目をもつ。第 3 者が通信情報を盗聴し、これを用いて第 2 の局を繰り返し攻撃したとしても、これは既に使用された乱数を用いた攻撃である。するとこの乱数は上記乱数履歴に存在するので、第 2 の局は、この攻撃を、第 3 者によるものと判断することができる。そのため第 3 者による不当な繰り返し攻撃を見つけることができるので、第 3 者による通信システムへのそれ以上の侵入を防止することができる。しかも、乱数認証において第 1 の局を正当でないと第 2 の局が判定した場合は、第 2 の局側での認証情報作成処理を省略できる。したがって、第 2 の局が第 3 者の攻撃により占有される程度を軽減することができる。

【0024】また、乱数が正当と判断された場合は、第 2 の局は第 2 の認証情報の生成と、第 1 および第 2 の認証情報の比較とを行なうので、正当な通信相手の認証は第 1 の発明と同様に正確におこなうことができる。

【0025】なお、この認証方法の第 2 の発明において情報を送信する各処理は、それぞれを別々に行なうことを必須とする意味ではない。通信回数を減らす意味から、情報処理に支障がない範囲で、いくつかの送信処理を同時に行ってももちろん良い。例えば、ユーザ情報、乱数および認証情報は同時に送信することができる。

【0026】この認証方法の第 2 の発明を実施するため、以下の(1)～(8)の手段を具えた通信システム（通信システムの第 2 の発明）を構成するのが好適である。

【0027】(1) 前記第 1 の局から前記第 2 の局に第 1 の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段。(2) 前記第 1 の局に設けられ、乱数を発生するための乱数生成手段。(3) 前記発生された乱数を前記第 2 の局に送信するための乱数送信手段。(4) 前記第 1 の局に設けられ、前記乱数と自局内の前記記憶手段に格納された前記秘密情報とを入力とする所定のアルゴリズムにより第 1 の認証情報を生成するための第 1 の認証情報生成手段。(5) 前記第 1 の認証情報を前記第 2 の局に送信するための認証情報送信手段。(6) 前記第 2 の局に設けられ、前記送信されてくる乱数を認証するため

の乱数認証手段。(7) 前記第2の局に設けられ、前記送信されてくる乱数と自局内の前記記憶手段に格納された前記秘密情報とを入力とする所定のアルゴリズムにより第2の認証情報を生成するための第2の認証情報生成手段。(8) 前記第2の局に設けられ、前記第1の認証情報と前記第2の認証情報とを比較することにより前記第1の局の正当性を認証するための認証手段。

【0028】(3)、また、この出願の認証方法の第3の発明によれば、共通の秘密情報をそれぞれの記憶手段に格納している第1の局および第2の局を含む通信システムにおいて、前記第2の局が前記第1の局を認証するに当たり、以下の各処理を含むことを特徴とする。

【0029】(a) 前記第1の局が、第1の局である旨を示すユーザ情報を第2の局に送信する処理。(b) 前記第1の局または第2の局が、乱数を発生してこれを他方の局に送信する処理。(c) 前記第1の局が、前記第2の局をアクセスした回数を計数すると共に該アクセス回数を前記第2の局に送信する処理。(d) 前記第1の局が、前記乱数と前記アクセス回数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより第1の認証情報を生成しこれを前記第2の局に送信する処理。(e) 前記第2の局が、前記送信されてきたアクセス回数を認証する処理。(f) 前記アクセス回数を認証する処理にて前記アクセス回数が正当でないとされた場合に実行され、前記第2の局が前記第1の局を正当でないとする処理。(g) 前記アクセス回数を認証する処理にて前記アクセス回数が正当であるとされた場合に実行され、前記第2の局が、前記乱数と前記アクセス回数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより第2の認証情報を生成し、かつ、前記第1の認証情報と前記第2の認証情報とを比較することにより前記第1の局の正当性を認証する処理。

【0030】この認証方法の第3の発明によれば、第1の局が第2の局にユーザ情報、乱数およびアクセス回数を送信すると認証動作が開始される。また認証は、第1の局から送信されてきたアクセス回数に対し先ず行なうことができる。アクセス回数の認証は、例えば、前回の送信の際に第1の局から送信されてきたアクセス回数を $n'a$ 、第1の局から今回送信されてきたアクセス回数を n_a 、通信ミスなどを考慮した数を ϵ としたとき、 $n'a + \epsilon > n_a > n'a$ という不等式関係を満たすか否かを調べるにより行なうことができる。

【0031】アクセス回数の認証は次の様な役目をもつ。第3者が通信情報を盗聴し、これを用いて第2の局を繰り返し攻撃したとしても、この攻撃で送信されてくるアクセス回数は既に送られてきた値と同じである。すると上記不等式関係を満たさないで、第2の局は、この攻撃を、第3者によるものと判断することができる。そのため第3者による不当な繰り返し攻撃を見つけるこ

とができるので、第3者による通信システムへのそれ以上の侵入を防止することができる。しかも、アクセス回数の認証において第1の局を正当でないと第2の局が判定した場合は、第2の局側での認証情報作成処理を省略できる。このため、第3者の攻撃により第2の局が占有される程度を軽減することができる。

【0032】また、上記の第2の発明では過去に使用した乱数を記憶する必要があるのに対し、この第3の発明ではアクセス回数を記憶するだけで済むので、第2の発明に比べメモリを節約することができる。

【0033】また、アクセス回数が正当と判断された場合は、第2の局は第2の認証情報の生成と、第1および第2の認証情報の比較とを行なうので、正当な通信相手の認証を正確におこなうことができる。

【0034】またこの第3の発明の場合では、認証情報は乱数、アクセス回数、秘密情報および所定のアルゴリズムにより生成するので、第1発明に比べさらに詳細な認証を行なうことができる。

【0035】なお、この認証方法の第3の発明を実施するに当たり、好ましくは第1の局が乱数を発生し第2の局に送信するのが良い。こうすると、ユーザ情報を送信する際に乱数も一緒に送信することができる。一方、第2の局が乱数を発生する手順にした場合は、第1の局側が認証情報を生成するために必須の乱数を第2の局から第1の局に別途に送信する処理が必要になるので、第1の局が乱数を発生する場合に比べて通信回数が増えてしまう。

【0036】この認証方法の第3の発明を実施するため、以下の(1)～(10)の手段を具えた通信システム(通信システムの第3の発明)を構成するのが好適である。

【0037】(1) 前記第1の局から前記第2の局に第1の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段。(2) 前記第1の局または前記第2の局に設けられ、乱数を発生するための乱数生成手段。(3) 前記発生された乱数を他方の局に送信するための乱数送信手段。(4) 前記第1の局に設けられ、前記第1の局が前記第2の局をアクセスしたアクセス回数を計数するためのアクセス回数計数手段。(5) 前記アクセス回数を前記第2の局に送信するためのアクセス回数送信手段。(6) 前記第1の局に設けられ、前記アクセス回数と前記乱数と自局内の前記記憶手段に格納された前記秘密情報とを入力とする所定のアルゴリズムにより第1の認証情報を生成するための第1の認証情報生成手段。(7) 前記第1の認証情報を前記第2の局に送信するための認証情報送信手段。(8) 前記第2の局に設けられ、前記送信されてくるアクセス回数を認証するためのアクセス回数認証手段。(9) 前記第2の局に設けられ、前記送信されてくるアクセス回数と乱数と自局内の前記記憶手段に格納された前記秘密情報とを入力とする所定のアルゴリズムにより第2の認証情報を生成するための第2の認証情報生成

手段。(10)前記第2の局に設けられ、前記第1の認証情報と前記第2の認証情報とを比較することで前記第1の局の正当性を認証するための認証手段。

【0038】(4)、また、この出願の認証方法の第4の発明によれば、共通の秘密情報をそれぞれの記憶手段に格納している第1の局および第2の局を含む通信システムにおいて、前記第2の局が前記第1の局を認証するに当たり、以下の各処理を含むことを特徴とする。

【0039】(a) 前記第1の局が、第1の局である旨を示すユーザ情報を前記第2の局に送信する処理。(b) 前記第1の局が、乱数を発生する処理。(c) 前記第1の局が、自局内の前記記憶手段に格納してある前記秘密情報を鍵として前記乱数と前記ユーザ情報とを暗号化することにより認証情報を生成しこれを前記第2の局に送信する処理。(d) 前記第2の局が、自局内の前記記憶手段に格納してある前記秘密情報を鍵として前記送信されてきた認証情報を復号化する処理。(e) 前記第2の局が、前記復号化で得たユーザ情報と前記送信されてきたユーザ情報とを比較すること、および、前記復号化で得た乱数を認証することにより前記第1の局の正当性を認証する処理。

【0040】この認証方法の第4の発明によれば、第1の局が第2の局にユーザ情報を送信すると認証動作が開始される。しかも、第1の局がユーザ情報および乱数を暗号化して第2の局に送り、第2の局はこれらを復号化しそれにより第1の局を認証する。暗号化および復号化を含むので、その分、認証方法自体が解読されにくいと考えられる。

【0041】また、この第4発明の場合も、第1の局が第2の局をアクセスするごとに乱数を発生している。この乱数は暗号化された状態で第2の局に送信され、そして第2の局で復号化される。復号化された乱数は認証される。乱数の認証は、例えば、今回復号された乱数が過去の通信の際に復号された乱数履歴に含まれているか否かを調べることにより行なうことが出来る。第3者が通信情報を盗聴してこれを用いて第2の局を攻撃してもこの通信情報から復号される乱数は既に使われた乱数である。すると第2の局は、この攻撃を、第3者によるものと判断することができる。すなわち、復号したユーザ情報のみの認証であると、第3者が通信情報を盗聴してそれを送ってきた場合に第3者が正当とされてしまうが、この第4の発明では復号した乱数をも認証するので、第3者の攻撃を防止することができる。

【0042】なお、この認証方法の第4の発明において情報を送信する各処理は、それぞれを別々に行なうことを必須とする意味ではない。通信回数を減らす意味から、情報処理に支障がない範囲で、いくつかの送信処理を同時に行ってももちろん良い。例えば、ユーザ情報、乱数および認証情報は同時に送信することができる。

【0043】この認証方法の第4の発明を実施するた

め、以下の(1)～(6)の手段を具えた通信システム(通信システムの第4の発明)を構成するのが好適である。

【0044】(1) 前記第1の局から前記第2の局に第1の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段。(2) 前記第1の局に設けられ、乱数を発生するための乱数生成手段。(3) 前記第1の局に設けられ、自局内の前記記憶手段に格納してある前記秘密情報を鍵として前記乱数と前記ユーザ情報とを暗号化することにより認証情報を生成するための認証情報生成手段。(4) 前記認証情報を前記第2の局に送信するための認証情報送信手段。(5) 前記第2の局に設けられ、自局内の前記記憶手段に格納してある前記秘密情報を鍵として前記送信されてくる認証情報を復号化するための認証情報復号化手段。(6) 前記第2の局に設けられ、前記復号化により得られたユーザ情報と前記送信されてくるユーザ情報とを比較すること、および、前記復号化により得られた乱数を認証することにより前記第1の局の正当性を認証するための認証手段。

【0045】(5)、また、この出願の認証方法の第5の発明によれば、共通の秘密情報をそれぞれの記憶手段に格納している第1の局および第2の局を含む通信システムにおいて、前記第2の局が前記第1の局を認証するに当たり、以下の各処理を含むことを特徴とする。

【0046】(a) 前記第1の局が、第1の局である旨を示すユーザ情報を前記第2の局に送信する処理。(b) 前記第1の局が、第1の乱数および第2の乱数を発生する処理。(c) 前記第1の局が、前記第1の乱数を前記第2の局に送信する処理。(d) 前記第1の局が、前記第2の乱数を鍵として前記ユーザ情報を暗号化して第1の暗号文を生成する処理。(e) 前記第1の局が、自局内の前記記憶手段に格納してある前記秘密情報と前記第1の乱数とを入力とする所定のアルゴリズムにより認証情報を生成するための暗号アルゴリズムの鍵を生成する処理。

(f) 前記第1の局が、前記暗号アルゴリズムの鍵を用いて前記第2の乱数と前記第1の暗号文とをさらに暗号化して第2の暗号文を生成しこれを認証情報として前記第2の局に送信する処理。(g) 前記第2の局が、前記送信されてきた第1の乱数を認証する処理。(h) 前記第1の乱数を認証する処理にて前記第1の乱数が正当でないとされた場合に実行され、前記第2の局が前記第1の局を正当でないとする処理。(i) 前記第1の乱数を認証する処理にて前記第1の乱数が正当であるとされた場合に実行され、前記第2の局が、自局内の前記記憶手段に格納してある前記秘密情報と前記第1の乱数とを入力とする所定のアルゴリズムにより認証情報を復号化するための鍵を生成し、該鍵を用い前記送信されてきた認証情報を復号化し、該復号化で得たユーザ情報と前記送信されてきたユーザ情報とを比較することにより前記第1の局の正当性を認証する処理。

【0047】この認証方法の第5の発明によれば、認証

動作において第1の乱数の認証を先ず行なうことができる。第1の乱数の認証は、例えば、上記の第2の発明の説明において説明したように乱数履歴を参照する方法で行なうことが出来る。そして、上記の第2の発明において説明した乱数を認証することの利点が、この第5の発明の場合も同様に得られる。

【0048】またこの認証方法の第5の発明では、本来の認証動作は次のように行なわれる。第1の局が第1の暗号文を生成しさらにこれを暗号化して認証情報を生成する。第2の局はこの認証情報を復号化しそしてこの復号化で得た情報により第2の局が第1の局を認証する。2重の暗号化を用いているので、上記の第4の発明に比べ認証方法自体がさらに解読されにくいと考えられる。また、認証情報の生成に用いる乱数を第1および第2の乱数としたので、認証情報の生成に用いる乱数が1つの場合より、認証方法自体が解読されにくいと考えられる。

【0049】なお、この認証方法の第5の発明において情報を送信する各処理は、それぞれを別々に行なうことを必須とする意味ではない。通信回数を減らす意味から、情報処理に支障がない範囲で、いくつかの送信処理を同時に行ってももちろん良い。

【0050】この認証方法の第5の発明を実施するため、以下の(1)～(11)の手段を具えた通信システム（通信システムの第5の発明）を構成するのが好適である。

【0051】(1) 前記第1の局から前記第2の局に対し第1の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段。(2) 前記第1の局に設けられ、第1の乱数および第2の乱数を発生するための乱数生成手段。(3) 前記発生された第1の乱数を前記第2の局に送信するための乱数送信手段。(4) 前記第1の局に設けられ、前記第2の乱数を鍵として前記ユーザ情報を暗号化して第1の暗号文を生成するための暗号文生成手段。(5) 前記第1の局に設けられ、前記第1の乱数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより認証情報を生成するための暗号アルゴリズムの鍵を生成するための暗号鍵生成手段。(6) 前記第1の局に設けられ、前記暗号アルゴリズムの鍵を用いて前記第2の乱数と前記第1の暗号文とをさらに暗号化して認証情報としての第2の暗号文を生成するための認証情報生成手段。(7) 前記認証情報を前記第2の局に送信するための認証情報送信手段。(8) 前記第2の局に設けられ、前記送信されてくる第1の乱数を認証するための乱数認証手段。(9) 前記第2の局に設けられ、前記送信されてくる第1の乱数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより前記認証情報を復号化するための鍵を生成するための復号鍵生成手段。(10) 前記第2の局に設けられ、前記復号鍵を用いて前記認証情報を復号化するための認証情報復号化手段。(11) 前記第2の局に設

けられ、前記復号化により得られたユーザ情報と前記送信されてくるユーザ情報とを比較することにより前記第1の局の正当性を認証するための認証手段。

【0052】(6)、また、この出願の認証方法の第6の発明によれば、共通の秘密情報をそれぞれの記憶手段に格納している第1の局および第2の局を含む通信システムにおいて、前記第2の局が前記第1の局を認証するに当たり、以下の各処理を含むことを特徴とする。

【0053】(a) 前記第1の局が、第1の局である旨を示すユーザ情報を前記第2の局に送信する処理。(b) 前記第1の局が、乱数を発生する処理。(c) 前記第1の局が、前記第2の局をアクセスした回数を計数する処理。(d) 前記第1の局が、前記乱数を鍵として前記ユーザ情報と前記アクセス回数とを暗号化する処理。(e) 前記第1の局が、自局内の前記記憶手段に格納してある前記秘密情報を鍵として前記暗号化されたユーザ情報と前記アクセス回数とをさらに暗号化してこれを認証情報として前記第2の局に送信する処理。(f) 前記第2の局が、自局内の前記記憶手段に記憶してある前記秘密情報を鍵として前記送信されてきた認証情報を復号化する処理。(g) 前記第2の局が、前記復号化で得たユーザ情報と前記送信されてきたユーザ情報とを比較すること、および、前記復号化で得たアクセス回数を認証することにより前記第1の局の正当性を認証する処理。

【0054】この認証方法の第6の発明によれば、第1の局が、乱数を鍵とする第1の暗号化と秘密情報を鍵とする第2の暗号化により認証情報を生成し、これを第2の局に送信する。一方、秘密情報自体は第2の局が自局の記憶手段に予め持っている。そのため第2の局は、第1の局から送信されてくる認証情報を、上記の秘密情報および乱数を鍵として復号することができる。そして復号化した情報により第1の局の正当性を認証する。しかも、ユーザ情報およびアクセス回数の両方を暗号化し、かつ、二重の暗号化をしているので、認証方法自体が解読されにくいと考えられる。

【0055】さらにこの認証方法の第6の発明では、復号したアクセス回数を認証する。アクセス回数の認証は、例えば上述したように、 $n'a + \epsilon > n_a > n'a$ という不等式関係を満たすか否かを調べることにより行なうことが出来る。第3者が通信情報を盗聴し、これを用いて第2の局を繰り返し攻撃したとしても、これは既に使用されたアクセス回数と同じ値を含む通信情報による攻撃である。すると上記不等式関係を満たさないので、第2の局は、この攻撃を、第3者によるものと判断することができる。

【0056】なお、この認証方法の第6の発明において情報を送信する各処理は、それぞれを別々に行なうことを必須とする意味ではない。通信回数を減らす意味から、情報処理に支障がない範囲で、いくつかの送信処理を同時に行ってももちろん良い。

【0057】この認証方法の第6の発明を実施するため、以下の(1)～(3)の手段を具えた通信システム(通信システムの第6の発明)を構成するのが好適である。

【0058】(1)前記第1の局から前記第2の局に対し第1の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段。(2)前記第1の局に設けられ、乱数を発生するための乱数生成手段。(3)前記第1の局に設けられ、前記第1の局が前記第2の局をアクセスしたアクセス回数を計数するためのアクセス回数計数手段。

(4)前記第1の局に設けられ、前記乱数を鍵として前記ユーザ情報と前記アクセス回数とを暗号化するための暗号化手段。(5)前記第1の局に設けられ、自局内の前記記憶手段に格納してある前記秘密情報を鍵として前記暗号化されたユーザ情報とアクセス回数とをさらに暗号化することにより認証情報を生成するための認証情報生成手段。(6)前記認証情報を前記第2の局に送信するための認証情報送信手段。(7)前記第2の局に設けられ、自局内の前記記憶手段に格納してある前記秘密情報を鍵として前記送信されてくる認証情報を復号化するための認証情報復号化手段。(8)前記第2の局に設けられ、前記復号化により得られるユーザ情報と前記送信されてくるユーザ情報とを比較すること、および、前記復号化により得られるアクセス回数を認証することにより前記第1の局の正当性を認証するための認証手段。

【0059】(7)、また、この出願の認証方法の第7の発明によれば、共通の秘密情報をそれぞれの記憶手段に格納している第1の局および第2の局を含む通信システムにおいて、前記第2の局が前記第1の局を認証するに当たり、以下の各処理を含むことを特徴とする。

【0060】(a)前記第1の局が、第1の局である旨を示すユーザ情報を前記第2の局に送信する処理。(b)前記第1の局が、第1の乱数および第2の乱数を発生する処理。(c)前記第1の局が、該第1の乱数を前記第2の局に送信する処理。(d)前記第1の局が、前記第2の局をアクセスした回数を計数する処理。(e)前記第1の局が、前記第2の乱数を鍵として前記ユーザ情報と前記アクセス回数とを暗号化して第1の暗号文を生成する処理。(f)前記第1の局が、自局内の前記記憶手段に格納してある前記秘密情報と前記第1の乱数とを入力とする所定のアルゴリズムにより認証情報を生成するための暗号アルゴリズムの鍵を生成する処理。(g)前記第1の局が、前記暗号アルゴリズムの鍵を用いて前記第2の乱数と前記第1の暗号文とをさらに暗号化して第2の暗号文を生成しこれを認証情報として前記第2の局に送信する処理。(h)前記第2の局が、自局内の前記記憶手段に格納してある前記秘密情報と前記第1の乱数とを入力とする所定のアルゴリズムにより前記認証情報を復号化するための鍵を生成する処理。(i)前記第2の局が、前記復号化するための鍵を用い前記送信されてきた認証情報を復号化する処理。(j)前記復号化で得たユーザ情報と

前記送信されてきたユーザ情報とを比較すること、および、前記復号化で得たアクセス回数を認証することにより前記第1の局の正当性を認証する処理。

【0061】この認証方法の第7の発明によれば、第1の局が、第2の乱数を鍵とし第1の暗号文を生成する。さらに第1の局が、秘密情報、第1の乱数および所定のアルゴリズムで暗号アルゴリズムの鍵を生成、この鍵を用い第1の暗号文をさらに暗号化して第2の暗号文を生成し、これを認証情報として第2の局に送信する。一方、第2の局には第1の局から第1の乱数が送信されており、かつ、秘密情報自体および所定のアルゴリズム自体は第2の局が予め持っている。そのため、第2の局は、これら第1の乱数、秘密情報および所定のアルゴリズムにより復号化するための鍵を生成できる。生成した復号化するための鍵を用い認証情報を復号化すると第2の乱数すなわち第1の暗号文を生成した際の鍵を復号することができる。この第2の乱数を鍵として用い認証情報を復号化すると、ユーザ情報とアクセス回数とを復号することができる。

【0062】この認証方法の第7の発明の場合、ユーザ情報およびアクセス回数の両方を暗号化し、然も二重の暗号化をし、然も認証情報生成のための暗号鍵および認証情報復号のための復号鍵それぞれを、秘密情報、第1の乱数および所定のアルゴリズムで生成しているので、上記の第6の発明に比べ、認証方法自体がさらに解読されにくいと考えられる。

【0063】さらにこの認証方法の第7の発明では、復号されたアクセス回数を認証する。アクセス回数の認証は、例えば上述したように、 $n'a + \epsilon > n_a > n'a$ という不等式関係を満たすか否かを調べることにより行なうことができる。第3者が通信情報を盗聴し、これを用いて第2の局を繰り返し攻撃したとしても、これは既に使用されたアクセス回数を用いた攻撃である。すると上記不等式関係を満たさないので、第2の局は、この攻撃を、第3者によるものと判断することができる。

【0064】なお、この認証方法の第7の発明において情報を送信する各処理は、それぞれを別々に行なうことを必須とする意味ではない。通信回数を減らす意味から、情報処理に支障がない範囲で、いくつかの送信処理を同時に行ってももちろん良い。

【0065】この認証方法の第7の発明を実施するため、以下の(1)～(11)の手段を具えた通信システム(通信システムの第7の発明)を構成するのが好適である。

【0066】(1)前記第1の局から前記第2の局に対し第1の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段。(2)前記第1の局に設けられ、第1の乱数および第2の乱数を発生するための乱数生成手段。(3)前記発生された第1の乱数を前記第2の局に送信するための乱数送信手段。(4)前記第1の局に設けられ、前記第1の局が前記第2の局をアクセスしたアクセ

ス回数を計数するためのアクセス回数計数手段。(5) 前記第 1 の局に設けられ、前記第 2 の乱数を鍵として前記ユーザ情報と前記アクセス回数とを暗号化して第 1 の暗号文を生成するための暗号文生成手段。(6) 前記第 1 の局に設けられ、前記第 1 の乱数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより認証情報を生成するための暗号アルゴリズムの鍵を生成するための暗号鍵生成手段。(7) 前記第 1 の局に設けられ、前記暗号アルゴリズムの鍵を用いて前記第 2 の乱数と前記第 1 の暗号文とをさらに暗号化して認証情報としての第 2 の暗号文を生成するための認証情報生成手段。(8) 前記認証情報を前記第 2 の局に送信するための認証情報送信手段。(9) 前記第 2 の局に設けられ、前記送信されてくる第 1 の乱数と自局内の前記記憶手段に格納してある前記秘密情報とを入力とする所定のアルゴリズムにより前記認証情報を復号化するための鍵を生成するための復号鍵生成手段。(10) 前記第 2 の局に設けられ、前記送信されてくる認証情報を前記復号鍵を用い復号化するための認証情報復号化手段。(11) 前記第 2 の局に設けられ、前記復号化により得られるユーザ情報と前記送信されてくるユーザ情報とを比較すること、および、前記復号化により得られるアクセス回数を認証することにより前記第 1 の局の正当性を認証するための認証手段。

【0067】上述した認証方法の第 1 ～第 7 の発明は、第 1 の局および第 2 の局間で直接通信を行ない認証を行なう例であった。しかし、通信システムでは、通信を希望する第 1 の局と第 2 の局との間に、第 1 の局の認証を第 2 の局に代わって行なう信頼できる第 3 の局が入ったり、中間局が入ることも多い。通信を希望する第 1 の局または第 2 の局の負荷を分散する等の目的からである、

認証方法の第 8 ～第 10 の各発明はその例である。

【0068】(8) . この出願の認証方法の第 8 の発明によれば、通信を希望する第 1 の局および第 2 の局と、該第 2 の局に代わって認証をする信頼できる第 3 の局とを含み、前記第 1 の局および第 3 の局は共通の秘密情報をそれぞれの記憶手段に格納している通信システムにおいて、前記第 3 の局が前記第 1 の局を実際に認証するに当たり、以下の各処理を含むことを特徴とする。

【0069】(a) 前記第 1 の局が、乱数を発生し、該乱数と第 1 の局である旨を示すユーザ情報とを前記第 2 の局に送信する処理。(b) 前記第 1 の局が、前記乱数と自局内の前記記憶手段に格納してある前記秘密情報とを用いて認証情報を生成しこれを前記第 2 の局に送信する処理。(c) 前記第 2 の局が、前記第 1 の局から送信されてきたユーザ情報と乱数と認証情報とを前記第 3 の局に送信する処理。(d) 前記第 3 の局が、前記第 2 の局から送信されてきた認証情報を前記乱数と自局内の前記記憶手段に格納してある前記秘密情報を用いて認証することにより前記第 1 の局の正当性を認証する処理。(e) 前記第

3 の局が前記第 2 の局に認証結果を送信する処理。

【0070】この認証方法の第 8 の発明によれば、第 2 の局は第 1 の局から送信されてきたユーザ情報と乱数と認証情報とを前記第 3 の局に送信し、第 3 の局に第 1 の局の認証をさせ、その結果を受信することが出来る。第 1 の局に対し共通の秘密情報を持たない第 2 の局であっても、第 2 の局は、第 1 の局が正当な通信者であるか否かを、第 2 の局が信頼する第 3 の局の力を借りて、認証することができる。そのため第 2 の局は安心して第 1 の局と通信をおこなうことができる。第 2 の局が認証動作しない分、第 2 の局の負荷が軽減される。

【0071】また認証方法の第 8 の発明の場合、第 1 の局で乱数を発生しているので、乱数をユーザ情報と一緒に第 2 の局に送信することができる。第 2 の局で乱数を発生した場合（後の認証方法の第 9 の発明）は、第 1 の局が認証情報生成に必要な乱数を第 2 の局が第 1 の局に送信する専用の処理が必要となるので通信回数が増えてしまう。この点を考えると、第 1 の局で乱数を発生するのが好ましい。

【0072】なお、この認証方法の第 8 の発明において認証情報の生成や認証情報の認証をいかなる方法で行なうかは、任意である。なぜなら、第 3 の局が含まれた場合に第 2 の局に変わって第 3 の局が第 1 の局を認証できるよう、第 1 ～第 3 の局間の情報の授受を工夫した点を特徴としているからである（以下の認証方法の第 9 の発明において同じ。）。ただし好ましくは、上記の認証方法の第 2 ～第 7 の発明で主張しているそれぞれの認証情報の生成手順、それぞれの認証情報の認証手順のいずれかを用いるのが良い（以下の認証方法の第 9 の発明において同じ。）。こうすると、第 3 の局が追加された場合でも、第 3 者（正当でない通信者）による繰り返り攻撃を防止できるという上記の効果が得られるからである。

【0073】この認証方法の第 8 の発明を実施するため、以下の各手段(1)～(8)を含む通信システム（通信システムの第 8 の発明）を構成するのが好適である。

【0074】(1) 前記第 1 の局から前記第 2 の局に第 1 の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段。(2) 前記第 1 の局に設けられ、乱数を発生するための乱数生成手段。(3) 前記発生された乱数を前記第 2 の局に送信するための乱数送信手段。(4) 前記第 1 の局に設けられ、前記乱数と自局内の前記記憶手段に格納された前記秘密情報とを用い認証情報を生成するための認証情報生成手段。(5) 前記認証情報を前記第 2 の局に送信するための認証情報送信手段。(6) 前記第 1 の局から前記第 2 の局に送信されてくる前記ユーザ情報、前記乱数および前記認証情報それぞれを前記第 3 の局に送信するための送信手段。(7) 前記第 3 の局に設けられ、前記第 2 の局から送信されてくる前記認証情報を自局内の前記記憶手段に格納してある前記秘密情報を用いて認証することにより前記第 1 の局の正当性を認

証するための認証手段。(8) 第3の局に設けられ、認証結果を第2の局に送信するための手段。

【0075】(9)、またこの出願の認証方法の第9の発明によれば、通信を希望する第1の局および第2の局と、該第2の局に代わって認証をする信頼できる第3の局とを含み、前記第1の局および第3の局は共通の秘密情報をそれぞれの記憶手段に格納している通信システムにおいて、前記第3の局が前記第1の局を認証するに当たり、以下の各処理を含むことを特徴とする。

【0076】(a) 前記第1の局が、第1の局である旨を示すユーザ情報を前記第2の局に送信する処理。(b) 前記第2の局が、前記ユーザ情報を受信すると乱数を発生し該乱数を前記第1の局に送信する処理。(c) 前記第1の局が、前記第2の局から送信されてきた乱数と自局内の前記記憶手段に格納している前記秘密情報とを用いて認証情報を生成しこれを前記第2の局に送信する処理。(d) 前記第2の局が、前記乱数と、前記第1の局から送信されてきたユーザ情報と認証情報とを前記第3の局に送信する処理。(e) 前記第3の局が、前記第2の局から送信されてきたユーザ情報と認証情報とを自局内の前記記憶手段に格納してある前記秘密情報を用いて認証することにより前記第1の局の正当性を認証する処理。(f) 前記第3の局が第2の局に認証結果を送信する処理。

【0077】この認証方法の第9の発明の場合も第8の発明と同様、第1の局に対し共通の秘密情報を持たない第2の局であっても、第2の局は、第1の局が正当な通信者であるか否かを、第2の局が信頼する第3の局の力を借りて、認証することができる。そのため第2の局は安心して第1の局と通信をおこなうことができる。

【0078】またこの場合第2の局側が乱数を発生するので、第2の局に対する繰り返し攻撃（正当でない通信）を防止することができる。

【0079】この認証方法の第9の発明を実施するため、以下の各手段(1)～(8)を含む通信システム（通信システムの第9の発明）を構成するのが好適である。

【0080】(1) 前記第1の局から前記第2の局に第1の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段。(2) 前記第2の局に設けられ、前記ユーザ情報を受信すると乱数を発生するための乱数生成手段。(3) 前記発生された乱数を前記第1の局に送信するための乱数送信手段。(4) 前記第1の局に設けられ、前記乱数と自局内の前記記憶手段に格納された前記秘密情報とを用い認証情報を生成するための認証情報生成手段。(5) 前記認証情報を前記第2の局に送信するための認証情報送信手段。(6) 前記乱数と前記第1の局から前記第2の局に送信されてくる前記ユーザ情報および前記認証情報を前記第3の局に送信するための送信手段。

(7) 前記第3の局に設けられ、前記第2の局から送信されてくる前記認証情報を自局内の前記記憶手段に格納してある前記秘密情報を用いて認証することにより前記第

1の局の正当性を認証するための認証手段。(8) 前記第3の局に設けられ、前記第2の局に認証結果を送信するための手段。

【0081】(10)、またこの出願の認証方法の第10の発明によれば、通信を希望する第1の局および第2の局と、これら局間に介在する中間局とを含み、前記第1の局および第2の局は共通の秘密情報をそれぞれの記憶手段に格納している通信システムにおいて、以下の各処理を含むことを特徴とする。

10 【0082】(a) 前記第1の局が、第1の局である旨を示すユーザ情報を前記中間局に送信する処理。(b) 前記中間局が、前記ユーザ情報を受信すると乱数を発生し該乱数を前記第1の局に送信する処理。(c) 前記第1の局が、前記中間局から送信されてきた乱数と自局内の前記記憶手段に格納している前記秘密情報とを用いて認証情報を生成しこれを前記中間局に送信する処理。(d) 前記中間局が、前記乱数と、前記第1の局から送信されてきたユーザ情報と認証情報とを前記第2の局に送信する処理。(e) 前記第2の局が、前記中間局から送信されてきた認証情報を自局内の前記記憶手段に格納している前記秘密情報を用いて認証することにより前記第1の局の正当性を認証する処理。

30 【0083】この認証方法の第10の発明によれば、中間局が第1の局および第2の局の中継処理を行なう。第1の局および第2の局間に秘密情報を共有しない中間局が介在した場合でも、第2の局は、第1の局が正当な通信者であるか否かを、認証することができる。そのため第2の局は安心して第1の局と通信をおこなうことができる。しかも、中間局が乱数発生処理を担うので、その分、第1の局および第2の局の負荷を軽減することができる。

【0084】なお、この認証方法の第10の発明において認証情報の生成や認証情報の認証をいかなる方法で行なうかは、任意である。なぜなら、中間局が含まれた場合でも第2の局が第1の局を認証できるよう、第1、第2および中間局の情報の授受を工夫した点を特徴としているからである。ただし好ましくは、上記の認証方法の第2～第7の発明で主張しているそれぞれの認証情報の生成手順、それぞれの認証情報の認証手順のいずれかを

40 用いるのが良いこうすると、中間局が追加された場合でも、第3者（正当でない通信者）による繰り返し攻撃を防止できるという上記の効果が得られるからである。

【0085】この認証方法の第10の発明を実施するため、以下の各手段(1)～(7)を含む通信システム（通信システムの第10の発明）を構成するのが好適である。

【0086】(1) 前記第1の局から前記中間局に第1の局である旨を示すユーザ情報を送信するためのユーザ情報送信手段。(2) 前記中間局に設けられ、前記ユーザ情報を受信すると乱数を発生するための乱数生成手段。

50 (3) 前記発生された乱数を前記第1の局に送信するため

の乱数送信手段。(4) 前記第1の局に設けられ、前記送信されてくる乱数と自局内の前記記憶手段に格納してある前記秘密情報とを用いて認証情報を生成するための認証情報生成手段。(5) 前記認証情報を前記中間局に送信するための認証情報送信手段。(6) 前記乱数と前記第1の局から前記中間局に送信されてくる前記ユーザ情報および前記認証情報を前記第2の局に送信するための送信手段。(7) 前記第2の局に設けられ、前記送信されてくる認証情報を自局内の前記記憶手段に格納してある前記秘密情報を用いて認証することにより前記第1の局の正当性を認証するための認証手段。

【0087】(A)、なお認証方法の第1～第3の各発明を実施するに当たり、前記第1の局および第2の局それぞれに、前記所定のアルゴリズムとして用いることができるアルゴリズムを複数種かつ同様に(同じ種類という趣旨)予め用意しておくのが好適である。しかも、前記第1および第2の局のいずれか一方が選択信号を発生し、これに応じ前記第1および第2の局が前記複数種のアルゴリズムの中から1つを選択し、該選択されたアルゴリズムにより前記第1の局は前記第1の認証情報を生成し、前記第2の局は前記第2の認証情報を生成するのが好適である。こうすると、アルゴリズムを変更できる分、認証情報の生成アルゴリズムが増えるので、認証方法が解読されにくくなる。そのため、機密保護能力に優れる通信システムを実現することができる。

【0088】なお、第1および第2の局それぞれに用意される複数種のアルゴリズムは、例えば両局で共通に番号付けした状態で記憶させたアルゴリズムとするのが良い。そして、番号を指定すると両局で同じアルゴリズムが選択されるようにするのが良い。(以下の(B)、(D)においても同様とするのが良い。)

【0089】(B)、また認証方法の第5および第7の各発明を実施するに当たり、前記第1の局および第2の局それぞれに、前記所定のアルゴリズムとして用いることができるアルゴリズムを複数種かつ同様に(同じ種類という趣旨)予め用意しておくのが好適である。しかも、前記第1および第2の局のいずれか一方が選択信号を発生し、これに応じ前記第1および第2の局が前記複数のアルゴリズムの中から1つを選択し、該選択されたアルゴリズムにより、前記第1の局は前記暗号アルゴリズムの鍵を生成し、前記第2の局は前記認証情報を復号化するための鍵を生成するのが好適である。こうすると、アルゴリズムを変更できる分、鍵の種類が増えるため認証情報の生成アルゴリズムが増えるので、認証方法が解読されにくくなる。そのため、機密保護能力に優れる通信システムを実現することができる。

【0090】(C)、また、認証情報を作成する際に用いる所定のアルゴリズムとして一方向性関数を用いるのが好適である。具体的には、認証方法の第1～第3の発明での第1および第2の認証情報をそれぞれ作成するた

めの所定アルゴリズム、第5および第7の発明で暗号アルゴリズムの鍵および復号化するための鍵それぞれを作成するための所定アルゴリズムとして、一方向性関数を用いるのが好適である。一方向性関数は一方向性ハッシュ関数(one-way hash function)、或は単にハッシュ関数とも呼ばれる。これは、 x から $f(x)$ を計算するのは容易であるが、 $f(x)$ から x を求めるのは極めて困難な関数 $f(x)$ である。一方向性関数を用いると、認証情報から秘密情報や乱数等が解読される危険性を低減することができる。

【0091】(D)、また認証方法の第4～第7の各発明を実施するに当たり、前記第1の局および第2の局それぞれに、前記認証情報を生成する際のアルゴリズムおよび前記認証情報を復号化する際のアルゴリズムとして用いることができる複数種の暗号アルゴリズムを同様(同じ種類という趣旨)に予め用意しておくのが好適である。しかも、前記第1および第2の局のいずれか一方が選択信号を発生し、これに応じ前記第1および第2の局が前記複数の暗号アルゴリズムの中から1つを選択し、該選択された暗号アルゴリズムにより、前記第1の局は前記認証情報を生成する暗号化をし、前記第2の局は前記認証情報を復号化するのが好適である。こうすると、暗号アルゴリズムを変更することができる分、認証情報の生成アルゴリズムが増えるので、認証方法が解読されにくくなる。そのため、機密保護能力に優れる通信システムを実現することができる。

【0092】(I)、またこの出願の暗号鍵共有方法の第1の発明によれば、：認証方法の第1～第3の発明のいずれかにより前記第1の局について認証をし、：該認証により正当とされた場合は前記第1の局および第2の局それぞれで前記乱数および前記秘密情報を入力とする所定の暗号鍵生成アルゴリズムにより共有暗号鍵をそれぞれ生成し、：これを前記第1および第2の局の共有暗号鍵とすることを特徴とする。

【0093】この暗号鍵共有方法の第1の発明によれば、第1の局が正当とされると引き続いて共有暗号鍵が生成されるので、第1の局の認証と共有暗号鍵の生成とを連続的に行なうことができる。然も、認証方法で用いた情報である乱数および秘密情報を用い暗号鍵を生成することができる。

【0094】この暗号鍵共有方法の第1の発明を実施するため、次のように通信システム(通信システムの第1の発明)を構成するのが好適である。すなわち、通信システムの第1～第3の発明のいずれかの構成に加え、前記第1の局および第2の局それぞれに設けられ、前記認証手段により前記第1の局が正当であるとされた場合に動作し、前記乱数および前記秘密情報を入力とする暗号鍵生成アルゴリズムにより共有暗号鍵を生成する共有暗号鍵生成手段をさらに具えた通信システム。

【0095】(II)、またこの出願の暗号鍵共有方法の

第2の発明によれば、：認証方法の第4または第6の発明により前記第1の局について認証をし、：該認証により正当とされた場合は前記第1の局および第2の局それぞれで前記乱数を入力とする所定の暗号鍵生成アルゴリズムにより共有暗号鍵をそれぞれ生成し、これを前記第1および第2の局の共有暗号鍵とすることを特徴とする。

【0096】この暗号鍵共有方法の第2の発明によれば、第1の局が正当とされると引き続いて共有暗号鍵が生成されるので、第1の局の認証と共有暗号鍵の生成とを連続的に行なうことができる。然も、認証方法で用いた乱数を用い暗号鍵を生成することができる。

【0097】この暗号鍵共有方法の第2の発明の発明を実施するため、次のように通信システム（通信システムの第12の発明）を構成するのが好適である。すなわち、通信システムの第4または第6の発明の構成に加え、前記第1の局および第2の局それぞれに設けられ、前記認証手段により前記第1の局が正当であるとされた場合に動作し、前記乱数を入力とする暗号鍵生成アルゴリズムにより共有暗号鍵を生成する共有暗号鍵生成手段をさらに具えた通信システム。

【0098】(III)。またこの出願の暗号鍵共有方法の第3の発明によれば、：認証方法の第5または第7の発明により前記第1の局について認証をし、：該認証により正当とされた場合は前記第1の局および第2の局それぞれで前記第2の乱数を入力とする所定の暗号鍵生成アルゴリズムにより共有暗号鍵をそれぞれ生成し、：これを前記第1および第2の局の共有暗号鍵とすることを特徴とする。

【0099】この暗号鍵共有方法の第3の発明によれば、第1の局が正当とされると引き続いて共有暗号鍵が生成されるので、第1の局の認証と共有暗号鍵の生成とを連続的に行なうことができる。然も、認証方法で用いた情報である第2の乱数を用い暗号鍵を生成することができる。

【0100】この暗号鍵共有方法の第3の発明の発明を実施するため、次のように通信システム（通信システムの第13の発明）を構成するのが好適である。すなわち、通信システムの第5または第7の発明の構成に加えて、前記第1の局および第2の局それぞれに設けられ、前記認証手段により前記第1の局が正当であるとされた場合に動作し、前記第2の乱数を入力とする暗号鍵生成アルゴリズムにより共有暗号鍵を生成する共有暗号鍵生成手段をさらに具えた通信システム。

【0101】なお、暗号鍵共有方法の第1～第3の発明を実施するに当たり、前記第1の局および第2の局それぞれに、前記所定の暗号鍵生成アルゴリズムとして用いることができるアルゴリズムを複数種かつ同様（同じ種類という趣旨）に予め用意しておく。そして、前記第1および第2の局のいずれか一方が選択信号を発生し、こ

れに応じ前記第1および第2の局が前記複数種の暗号鍵生成アルゴリズムの中から1つを選択し、該選択された暗号鍵生成アルゴリズムにより、前記第1の局および第2の局は共有暗号鍵をそれぞれ生成するのが好適である。こうすると、暗号鍵生成アルゴリズムが増えるので、暗号鍵が解読されにくくなる。そのため、機密保護能力に優れる通信システムを実現することができる。

【0102】(IV)。またこの出願の暗号鍵共有方法の第4の発明によれば、：認証方法の第8または第9の発明により前記第1の局について認証をし、：該認証により正当とされた場合は前記第1の局および第3の局それぞれで共有暗号鍵をそれぞれ生成し、：前記第3の局は該共有暗号鍵を前記第2の局に送信しこれを前記第2の局は共有暗号鍵とすることを特徴とする。

【0103】この暗号鍵共有方法の第4の発明によれば、第1の局が正当とされると引き続いて共有暗号鍵が生成されるので、第1の局の認証と共有暗号鍵の生成とを連続的に行なうことができる。

【0104】この暗号鍵共有方法の第4の発明の発明を実施するため、次のように通信システム（通信システムの第14の発明）を構成するのが好適である。すなわち、通信システムの第8または第9の発明の構成に加えて、前記第1の局および第3の局それぞれに設けられかつ前記認証手段により前記第1の局が正当であるとされた場合に動作する共有暗号鍵生成手段と、前記第3の局で生成された共有暗号鍵を前記第2の局に送信するための共有暗号鍵送信手段とをさらに具えた通信システム。

【0105】(V)。またこの出願の暗号鍵共有方法の第5の発明によれば、：認証方法の第10の発明により前記第1の局について認証をし、：該認証により正当とされた場合は前記第1の局および第2の局それぞれで共有暗号鍵をそれぞれ生成し、：これを前記第1および第2の局の共有暗号鍵とすることを特徴とする。

【0106】この暗号鍵共有方法の第5の発明によれば、第1の局が正当とされると引き続いて共有暗号鍵が生成されるので、第1の局の認証と共有暗号鍵の生成とを連続的に行なうことができる。

【0107】この暗号鍵共有方法の第5の発明の発明を実施するため、次のように通信システム（通信システムの第15の発明）を構成するのが好適である。すなわち、通信システムの第10の発明の構成に加えて、前記第1の局および第2の局それぞれに設けられ、前記認証手段により前記第1の局が正当であるとされた場合に動作する共有暗号鍵生成手段をさらに具えた通信システム。

【0108】なお、通信システムの発明を実施するに当たり、特に、以下のように構成するのが好適である。

【0109】(i) 通信システムの第2の発明を実施するに当たり、前記乱数認証手段を、前記乱数が正当でないと判断した場合、前記第1の局を正当でないと決定する

10

20

30

40

50

手段とするのが好適である。しかも、前記第2の認証情報生成手段および前記認証手段それぞれを、前記乱数認証手段が前記乱数を正当と判断した場合に動作する手段とするのが好適である。こうすると第2の認証情報生成手段および認証手段の必要以上の動作を防止することができるので、通信システムの処理能力の向上、混雑緩和などが図れる。

【0110】(ii) 通信システムの第3の発明を実施するに当たり、前記アクセス回数認証手段を、前記アクセス回数が正当でないと判断した場合、前記第1の局を正当でないと決定する手段とするのが好適である。しかも、前記第2の認証情報生成手段および前記認証手段それぞれを、前記アクセス回数認証手段が前記アクセス回数を正当と判断した場合に動作する手段とするのが好適である。こうすると第2の認証情報生成手段および認証手段の必要以上の動作を防止することができるので、通信システムの処理能力の向上、混雑緩和などが図れる。

【0111】(iii) 通信システムの第5の発明を実施するに当たり、前記第1の乱数認証手段を、前記第1の乱数が正当でないと判断した場合、前記第1の局を正当でないと決定する手段とするのが好適である。しかも、前記復号鍵生成手段、前記認証情報復号化手段および前記認証手段それぞれを、前記第1の乱数認証手段が前記第1の乱数を正当と判断した場合に動作する手段とするのが好適である。こうすると、復号鍵生成手段、認証情報復号化手段および認証手段それぞれの必要以上の動作を防止することができるので、通信システムの処理能力の向上、混雑緩和などが図れる。

【0112】

【発明の実施の形態】以下、図面を参照してこの出願の各発明の実施の形態について説明する。しかしながら、説明に用いる各図はこれら発明を理解出来る程度に概略的に示してある。また、各図において同様な構成成分については同一の番号を付して示し、その重複する説明を省略することもある。

【0113】なお、この出願でいう第1の局、第2の局、第3の局および中間局それぞれを、コンピュータで構成することができる。また、各局は、通信回線により接続されることにより通信システムを構成する。通信プロトコルは任意のプロトコルとすることができる。また、これら発明でいう、認証情報生成手段、認証手段などの各手段は、コンピュータに備わるCPU、メモリ、インタフェース回路等およびコンピュータ間を接続している通信回線を組み合わせることにより構成することができる。

【0114】1. 第1の実施の形態

先ず、認証方法の第1の発明、暗号鍵共有方法の第1の発明、通信システムの第1および第11の発明それぞれの実施の形態を、併せて説明する。

【0115】1-1. 通信システムの構成説明

図1は第1の実施の形態の通信システムの構成を説明するための図である。

【0116】第1の局11は、秘密情報格納部13と、ユーザ情報格納部15と、送受信インタフェース17と、所定のアルゴリズムを複数格納する手段19（関数fテーブル19という）と、第1の認証情報生成手段21（f演算部21ともいう）と、共有鍵生成手段23と、暗号鍵生成アルゴリズムを複数格納する手段25（関数gテーブル25という）と、共有鍵格納部27とを具える。

【0117】ここで、秘密情報格納部13は、第1の局および第2の局で共通の秘密情報 K_a を記憶するための記憶手段である。この秘密情報格納部13は、認証情報生成手段21と共有鍵生成手段23とに接続してある、認証情報生成手段21と共有鍵生成手段23とは、秘密情報を、秘密情報格納部13から必要に応じ読み出すことができる。

【0118】ユーザ情報格納部15は、第1の局11についてのユーザ情報 I_a を格納するための記憶手段である。このユーザ情報格納部15は、送受信インタフェース17と接続してあり、必要に応じ他の局（ここでは第1の局）にユーザ情報を送信することができる。

【0119】送受信インタフェース17は、通信回線（図1の場合は100）と第2の局41の送受信インタフェース45と協力して、この発明でいう各種の送信手段を構成する。

【0120】関数fテーブル19は、詳細は後述するが、第1の認証情報生成手段21が第1の認証情報を生成する際に用いる所定のアルゴリズムを、複数格納するための記憶手段である。この関数fテーブル19は、第1の認証情報生成手段21と、送受信インタフェース17とに接続してある。

【0121】第1の認証情報生成手段21は、詳細は後述するが、第1の認証情報を生成するための手段である。この第1の認証情報生成手段21は、その秘密情報格納部13から秘密情報を入力し、認証情報を送受信インタフェース17に出力できるように、構成成分13、17と接続してある。

【0122】共有鍵生成手段23は、詳細は後述するが、認証処理にて第1の局が正当とされた場合、共有暗号鍵を生成するための手段である。

【0123】関数gテーブル25は、詳細は後述するが、共有暗号鍵生成手段23が暗号鍵を生成する際に用いる暗号鍵生成アルゴリズムを複数格納するための記憶手段である。この関数gテーブル25は、共有暗号鍵生成手段23と、送受信インタフェース17とに接続してある。

【0124】共有鍵格納部27は、共有生成手段23で生成された共有暗号鍵を格納するための手段である。

【0125】一方、第2の局41は、ユーザ情報・秘密

情報格納部43と、送受信インタフェース45と、所定のアルゴリズムを複数格納する手段47（関数fテーブル47）と、乱数生成手段49と、第2の認証情報生成手段51（f演算部51ともいう）と、共有鍵生成手段53と、暗号鍵生成アルゴリズムを複数格納する手段55（関数gテーブル55ともいう）と、共有鍵格納部57と、認証手段59とを具えている。

【0126】ここで、ユーザ情報・秘密情報格納部43は、正当な通信者ごとに、ユーザ情報 I_a と秘密情報 K'_a とを格納する記憶手段である。このユーザ情報・秘密情報格納部43は、送受信インタフェース45と、第2の認証情報生成手段51と、共有鍵生成手段53とにそれぞれ接続してある。第2の局41は、第1の局11からユーザ情報 I_a が送信されてくると、このユーザ情報 I_a により、ユーザ情報・秘密情報格納部43から対応する秘密情報 K'_a を検出することができる。

【0127】なお、秘密情報 K_a 、 K'_a は同じものであるが、どちらの局側の秘密情報かを区別するために、 K_a 、 K'_a と示している。

【0128】送受信インタフェース45は、第1の局11側の送受信インタフェース同様、この発明でいう各種の送信手段の構成成分の1つである。

【0129】関数fテーブル47は、詳細は後述するが、第2の認証情報生成手段51が第2の認証情報を生成する際に用いる所定のアルゴリズムを複数格納するための記憶手段である。この関数fテーブル51は、第2の認証情報生成手段51と、送受信インタフェース45とに接続してある。

【0130】乱数生成手段49は、第1の局11からユーザ情報 I_a を受信すると、乱数 r を発生するための手段である。この乱数生成手段49は、送受信インタフェース45と、第2の認証情報生成手段51と、共有鍵生成手段53とにそれぞれ接続している。しかも発生された乱数 r は第1の局11側の、第1の認証情報生成手段21と、共有鍵生成手段23にも送信される。なお、乱数生成手段49を第1の局11側に設け、第2の局41に第1の局11から乱数 r を送信するようにしても良い。

【0131】第2の認証情報生成手段51は、詳細は後述するが、第2の認証情報を生成するための手段である。この第2の認証情報生成手段51は、その出力を認証手段59に接続してある。

【0132】共有鍵生成手段53は、詳細は後述するが、認証処理にて第1の局が正当とされた場合、共有暗号鍵を生成するための手段である。

【0133】関数gテーブル55は、詳細は後述するが、共有暗号鍵生成手段53が暗号鍵を生成する際に用いる暗号鍵生成アルゴリズムを複数格納するための記憶手段である。この関数gテーブル55は、共有暗号鍵生成手段53と、送受信インタフェース45とに接続して

ある。

【0134】共有鍵格納部57は、共有生成手段23で生成された共有暗号鍵を格納するための手段である。

【0135】認証手段59は、第1の認証情報と第2の認証情報とを比較してその結果に応じ第1の局が正当であるか否かを認証する手段である。ここでは認証手段59を第1の認証情報と第2の認証情報とを比較する比較部で構成してある。

【0136】次に、いままでの説明で説明を簡単に済ませた構成成分について詳細に説明する。

【0137】まず、第1の認証情報生成手段21は、秘密情報 K_a と乱数 r と所定のアルゴリズムとから第1の認証情報を生成する。第2の認証情報生成手段51は、秘密情報 K'_a （ $=K_a$ ）と乱数 r と所定のアルゴリズムとから第2の認証情報を生成する。

【0138】この実施の形態では第1および第2の認証情報を生成するときに用いる所定のアルゴリズムとして、一方向性関数 f_i を用いる。したがって、第1の認証情報生成手段21は、一方向性関数 f_i と、乱数 r と、秘密情報 K_a とを用い第1の認証情報 $f_i(r, K_a)$ を生成する。一方、第2の認証情報生成手段51は、一方向性関数 f_i と、乱数 r と、秘密情報 K'_a とを用い第2の認証情報 $f_i(r, K'_a)$ を生成する。

【0139】しかもこの実施の形態では、一方向性関数 f_i は、第1の認証情報生成手段21については関数fテーブル19から、また、第2の認証情報生成手段51については関数fテーブル47から、それぞれ入力される構成としてある。

【0140】なお一方向性関数は、一方向性ハッシュ関数(one-way hash function)、或は単にハッシュ関数とも呼ばれる。一方向性関数とは簡単にいうと、 x から $f(x)$ を計算するのは容易であるが、 $f(x)$ から x を求めるのは極めて困難な関数 $f(x)$ である。

【0141】一方向性関数の具体例として、MD5(R. Rivest: The MD5 Message-Digest Algorithm, Networking Group, RFC 1321, 1992)やSHA(National Institute of Standards and Technology: Secure Hash Standard, FIPS PUB 180-1, 1995)などを挙げることができる。

【0142】また関数fテーブル19、47それぞれには、複数の一方向性関数 f_i を同じ種類それぞれ格納してある。しかも、格納した各関数に、両局で共通の番号を付してある。各関数fテーブル19、47に対し同じ番号 i （例えば $i=1, 2, 3, \dots$ のいずれか）を入力することで、各関数fテーブル19、47から、同じ一方向性関数を選択することができる。

【0143】なお、一方向性関数選択番号 i は、例えば第1の局11の通信開始信号に応じて第1の局11または第2の局41が、例えば乱数を用いたり、予め用意されたプログラムに従い、生成する。第1の局11および第2の局41のいずれが番号 i を生成するかは、通信シス

テムの設計に応じ決めるのが良い。この第1の実施の形態の場合は、第2の局41側で番号iを生成している。

【0144】一方向性関数を上記のMD5等とした場合、関数fテーブル19、47それぞれを、例えば、1. f_1 : MD5 2. f_2 : SHA 3. f_3 : HMAC-MD5 4. f_4 : HMAC-SHA 5. ... のようにすることができる。

【0145】なお、関数fテーブルを用いることなく、第1の局11および第2の局41に共通な1つの一方向性関数を、認証情報生成のための所定のアルゴリズムとする場合があっても良い。

【0146】また関数gテーブル25、55それぞれには、共有暗号鍵の生成に用いることができる暗号鍵生成アルゴリズム g_j （一方向性関数とは限らない。）を、同じ種類それぞれ格納してある。しかも、格納した各関数に、両局で共通の番号を付してある。各関数gテーブル25、55に対し同じ番号j（例えばj=1、2、3、...のいずれか）を入力することで、各関数gテーブル25、55から、同じ暗号鍵生成アルゴリズムを選択することができる。

【0147】なお、関数gテーブル25、55から関数を選択するための選択番号jは、例えば第1の局11の通信開始信号に応じて第1の局11または第2の局41に備わる例えばCPU（図示せず）が、乱数を用いたり、予め用意されたプログラムに従い、生成する。この第1の実施の形態では第2の局41側が選択番号jを生成することとしている。

【0148】ここで関数gテーブル25、55それぞれに格納する関数 g_j は、通信局間相互で決める任意好適なものとする。例えば $g(x)=X$ や $g(x)=S^n(x)$ （左n-巡回シフト）などを挙げることができる。その場合、関数gテーブルとして、1. $g_1(x)=X$ 2. $g_2(x)=S^n(x)$ （左n-巡回シフト） 3. ...等が考えられる。

【0149】なお、関数gテーブルを用いることなく、第1の局11および第2の局41に共通な1つのアルゴリズムを、共有暗号鍵生成のための所定のアルゴリズムとする場合があっても良い。

【0150】また共有鍵生成手段23は、第1の局11が正当であるとされた場合、認証方法で用いた情報のうちの1または複数と、関数gテーブル25から選択された関数 g_j とにより、共有暗号鍵化を生成する。この第1の実施の形態では、乱数rと、秘密情報 K_a と、関数gテーブル25から選択された関数 g_j とにより、共有暗号鍵化 $g_j(r, K_a)$ を生成する。生成された共有暗号鍵 $g_j(r, K_a)$ を、共有鍵格納部27は内部に格納する。

【0151】また、共有鍵生成手段53は、第1の局11が正当であるとされた場合、認証方法で用いた情報のうちの1または複数と、関数gテーブル55から選択さ

れた関数 g_j とにより、共有暗号鍵化を生成する。この第1の実施の形態では乱数rと、秘密情報 K_a と、関数gテーブル55から選択された関数 g_j とにより、共有暗号鍵化 $g_j(r, K_a)$ を生成する。生成された共有暗号鍵 $g_j(r, K_a)$ を、共有鍵格納部57は内部に格納する。

【0152】なお以下の他の実施の形態では、共有暗号鍵の生成のために用いる情報が、乱数rや秘密情報 K_a でなく、乱数rのみの場合や、第2の乱数 r_2 のみの場合等がある。しかし、以下の実施の形態の各説明図では共有鍵生成手段には共通に23、53という番号を付している。

【0153】1-2. 動作の説明

次に、第1の実施の形態の通信システムの動作を説明する。これにより、認証方法および共有暗号鍵の生成方法の処理手順を説明する。この説明を図1に加えて図2を参照して行なう。図2は処理の流れを示した図である。

【0154】第1の局11は、ユーザ情報 I_a を第2の局41に送信する（図2の通信101）。

【0155】ユーザ情報 I_a を受信した第2の局41は、乱数生成手段49を用いて乱数rを生成し、これを第1の局に返信する（図2の通信102）。なお、認証情報の生成に使う一方向性関数 f_i を指定する場合、第2の局41は、乱数rと共に関数番号iも第1の局11に送信する。また一方向性関数を指定しないときは事前に決められた関数を両局11、41は使うことになる。

【0156】次に、第1の局11は、乱数rと自分のもつ秘密情報 K_a とを使い、かつ、指定された或は事前に決められた一方向性関数 f_i を用いて、第1の認証情報 $f_i(r, K_a)$ を計算し（図2の処理111）、これを第2の局41の認証手段59に送信する（図2の通信103）。

【0157】第1の認証情報 $f_i(r, K_a)$ を受信した第2の局41は、次に、ユーザ情報 I_a に対応する秘密情報 K'_a を、ユーザ情報・秘密情報格納部43から見つけ出す。さらに第2の局41は、乱数rと秘密情報 K'_a とを使い、かつ、番号iに対応する一方向性関数 f_i を用いて、第2の認証情報 $f_i(r, K'_a)$ を計算し（図2の処理112）、これを認証手段（比較部）59に入力する。

【0158】次に、認証手段59は、第1の認証情報 $f_i(r, K_a)$ と、第2の認証情報 $f_i(r, K'_a)$ とを比較する（図2の処理113）。この比較で両者が等しければ、第2の局41は第1の局11の正当性を認め、そして通信許可信号"OK"と共有暗号鍵生成のための関数 g_i の番号jとを、第1の局11に送信する（図2の通信104）。また、第2の局41の共有鍵生成手段53は、共有暗号鍵を $K_{12}=g_j(r, K'_a)$ のように生成する（図2の処理114）。

【0159】一方、通信許可信号”OK”を受信した第1の局11は、共有鍵生成手段23を用いて共有暗号鍵を

$$K_{12} = g_j (r, K_a)$$

のように生成する（図2の処理115）。

【0160】この第1の実施の形態によれば、ユーザ情報と第三者に知られていたい秘密情報とを用いて、第2の局が第1の局の正当性を認証することができる。しかも、認証の際に用いた情報である乱数および秘密情報をそのまま用いて第1の局および第2の局の間に暗号鍵の共有を実現している。しかも、第1の局の認証処理と、第1の局および第2の局の間の共有暗号鍵の生成処理とを連続的に行なうことができる。

【0161】2. 第2の実施の形態

次に、認証方法の第2の発明、暗号鍵共有方法の第1の発明、通信システムの第2および第11の発明それぞれの実施の形態を、併せて説明する。

【0162】2-1. 通信システムの構成説明

図3は第2の実施の形態の通信システムの構成を説明する図である。

【0163】この第2の実施の形態の第1の実施の形態との主な相違点は、第2の局41側に設けていた乱数生成手段49を省略し、その代わりに第1の局11側に乱数生成手段29を設けた点と、第2の局41内に乱数認証手段61を設けた点と、第2の局41にユーザ情報・乱数履歴情報・秘密情報格納部63を設けた点である。

【0164】ここで、乱数生成手段29は、第1の認証情報生成手段21と、共有鍵生成手段23と、送受信インターフェース17とに接続してある。また発生された乱数 r は第2の局41側の、第2の認証情報生成手段51と、共有鍵生成手段53にも送信される。

【0165】ユーザ情報・乱数履歴情報・秘密情報格納部63は、ユーザ情報 I_a および秘密情報 K'_a を記憶していると共に、正当な通信者ごとの通信で使用された乱数 r を通信の度に記憶する（乱数履歴を記憶する）記憶手段である。このユーザ情報・乱数履歴情報・秘密情報格納部63は、送受信インターフェース17と、乱数認証手段61と、第1の認証情報生成手段51とに接続してある。

【0166】また、乱数認証手段61は、第1の局から送信されてくる乱数 r が、過去に送信されてきた乱数であるか否かを、通信が行なわれる度に、ユーザ情報・乱数履歴情報・秘密情報格納部63を検索して判定する手段である。この乱数認証手段61をここでは比較部61で構成してある。この乱数認証手段61は、送受信インターフェース45とユーザ情報・乱数履歴情報・秘密情報格納部63とに接続してある。

【0167】この第2の実施の形態の通信システムでは、乱数生成手段29、乱数認証手段61およびユーザ

情報・乱数履歴情報・秘密情報格納部63以外の構成は、第1の実施の形態と同じとしてある。

【0168】2-2. 動作の説明

次に、第2の実施の形態の通信システムの動作を説明する。これにより、認証方法および共有暗号鍵の生成方法の処理手順を説明する。この説明を図3に加えて図4を参照して行なう。図4は処理の流れを示した図である。

【0169】第1の局11の乱数生成手段29は通信のごとに異なる乱数 r を生成する。第1の局11の第1の認証情報生成部21は、この乱数 r と、秘密情報 K_a と、一方向性関数 f_i とにより、第1の認証情報 $f_i(r, K_a)$ を計算する（図4の処理211）。

【0170】次に、第1の局11は、第2の局41に、ユーザ情報 I_a と、乱数 r と、一方向性関数番号 i と、第1の認証情報 $f_i(r, K_a)$ とを送信する（図4の通信201）。

【0171】次に、第2の局41は、ユーザ情報 I_a を用いて、第1の局11についての乱数履歴と秘密情報 K'_a とを、ユーザ情報・乱数履歴情報・秘密情報格納部63から見つけ出す。次にまず、第2の局41の乱数認証手段61が、乱数履歴を調べて（図4の処理212）、もし受信した乱数 r が乱数履歴に入っているならば第1の局11の正当性を認めない。

【0172】乱数履歴を調べた結果、第1の局11の正当性を認めないこととなった場合は、第2の局41は認証動作を中止する。そして第2の局41は、通信を終了させたり、第1の局11にエラーメッセージを出す等任意好適な処置をとる。

【0173】一方、今回送信されてきた乱数が乱数履歴に含まれていなかった場合は、第2の局41の第2の認証情報生成手段51が、この乱数 r と秘密情報 K'_a と一方向性関数 f_i とを用いて第2の認証情報 $f_i(r, K'_a)$ を計算する（図4の処理213）。また、第2の局41は今回送信されてきた乱数 r を、ユーザ情報・乱数履歴情報・秘密情報格納部63に、乱数履歴情報として追加する。

【0174】次に、第2の局41の認証手段59は、第1の認証情報 $f_i(r, K_a)$ と第2の認証情報 $f_i(r, K'_a)$ とを比較する（図4の処理214）。この比較において両者が等しければ、第2の局41は、第1の局11の正当性を認め、通信許可信号”OK”と共有暗号鍵生成のための関数 g_j の番号 j とを、第1の局11に送信する（図4の通信202）。また、第2の局41の共有鍵生成手段53は、共有暗号鍵を $K_{12} = g_j(r, K'_a)$ のように生成する（図4の処理215）。

【0175】一方、通信許可信号”OK”を受信した第1の局11は、共有鍵生成手段23を用いて共有暗号鍵を $K_{12} = g_j(r, K_a)$ のように生成する（図4の処理216）。

【0176】この第2の実施の形態によれば、ユーザ情報と第三者に知られていない秘密情報とを用いて、第2の局が第1の局の正当性を認証することができる。しかも、認証の際に用いた情報である乱数および秘密情報をそのまま用いて第1の局および第2の局の間に暗号鍵の共有を実現している。しかも、第1の局の認証処理と、第1の局および第2の局の間の共有暗号鍵の生成処理とを連続的に行なうことができる。

【0177】また送信されてきた乱数が乱数履歴に含まれるか否かで、第1の局の正当性を判断することができる。そのため、正当でない通信者による繰り返し攻撃を止することができる。

【0178】また、第1の局が正当であることの認証は、第1の実施の形態と同様に行なうことができるので、安全性も確保できる。

【0179】またこの第2の実施の形態の方が、第1の実施の形態の場合に比べ、通信回数を少なくすることができる。

【0180】3. 第3の実施の形態

次に、認証方法の第3の発明、暗号鍵共有方法の第1の発明、通信システムの第3および第11の発明それぞれの実施の形態を、併せて説明する。

【0181】3-1. 通信システムの構成説明

図5は第3の実施の形態の通信システムの構成を説明する図である。

【0182】この第3の実施の形態の第1の実施の形態との主な相違点は、第2の局41側に設けていた乱数生成手段49を省略し、第2の実施の形態と同じく第1の局11側に乱数生成手段29を設けた点と、第2の局41内にアクセス回数認証手段65を設けた点と、第2の局41にユーザ情報・アクセス回数・秘密情報格納部67を設けた点と、第1の局11に第1の局11が第2の局41をアクセスするごとにアクセス回数を計数するアクセス回数計数手段31を設けた点である。

【0183】なお、乱数生成手段を第2の局41側に設ける場合があっても良い。しかし、第1の局11側に乱数生成手段を設けると、乱数とユーザ情報とを一緒に第2の局41に送信出来るので、通信回数を少なくすることができる。

【0184】ここでアクセス回数計数手段31は、第1の局11が第2の局41をアクセスする度にアクセス回数を計数する手段である。このアクセス回数計数手段31は、送受信インタフェース17と、第1の認証情報生成手段21とに接続してある。

【0185】このアクセス回数計数手段31は、第1の局11が第2の局41をアクセスするごとに例えば単調増加するカウンタにより構成することができる。なお、アクセス回数計数手段31で計数されたアクセス回数 n_a は、送受信インタフェース17、45と通信回線10

0とを介して、第2の局41のアクセス回数認証手段65に送信される。

【0186】またアクセス回数認証手段65は、第1の局11から送信されてくるアクセス回数 n_a が、第1の局からの過去のアクセス回数に対し正当な範囲にあるか否かを判定することでアクセス回数を認証する手段である。このアクセス回数認証手段65は、ユーザ情報・アクセス回数・秘密情報格納部63と、送受信インタフェース45とに接続してある。

【0187】このアクセス回数認証手段65は、この実施の形態では、第1の局11から今回送信されてきたアクセス回数を n_a 、ユーザ情報・アクセス回数・秘密情報格納部67に格納されている第1の局の前の通信までのアクセス回数を n'_a 、通信ミスを許容する許容値を ϵ （例えば5程度）としたとき、 n_a について $n'_a + \epsilon > n_a > n'_a$ という不等式関係が成立するか否かをチェックする比較部としてある。

【0188】またユーザ情報・アクセス回数・秘密情報格納部63は、ユーザ情報 I_a および秘密情報 K'_a を記憶していると共に、アクセス回数認証手段65が正当と認証したアクセス回数 n_a をその都度アクセス回数 n'_a として更新記憶する記憶手段である。このユーザ情報・アクセス回数・秘密情報格納部63は、送受信インタフェース45と、第2の認証情報生成手段51と、共有鍵生成手段53と、アクセス回数認証手段65とに接続してある。

【0189】この第3の実施の形態の通信システムでは、乱数生成手段29、アクセス回数計数手段31、アクセス回数認証手段65およびユーザ情報・アクセス回数・秘密情報格納部67以外の構成は、第1の実施の形態と同じとしてある。ただし、第1の認証情報生成手段21と第2の認証情報生成手段51は、この場合、乱数 r と、アクセス回数 n_a (n'_a)と、秘密情報 K_a (K'_a)と、一方向性関数 f_i とにより、第1および第2の認証情報を生成する構成としてある。

【0190】3-2. 動作の説明

次に、第3の実施の形態の通信システムの動作を説明する。これにより、認証方法および共有暗号鍵の生成方法の処理手順を説明する。この説明を図5に加えて図6を参照して行なう。図6は処理の流れを示した図である。

【0191】第1の局11の乱数生成手段29は、通信の際乱数 r を生成する。第1の局11のアクセス回数計数手段31は、計数値すなわちアクセス回数 n_a を1増加させ、 $n_a = n_a + 1$ とする。第1の局11の第1の認証情報生成部21は、乱数 r と、秘密情報 K_a と、アクセス回数 n_a とを使い、かつ、一方向性関数 f_i を用いて、第1の認証情報 $f_i(r, n_a, K_a)$ を計算する(図6の処理311)。

【0192】次に、第1の局11は、第2の局41に、ユーザ情報 I_a と、乱数 r と、一方向性関数番号 i と、

アクセス回数 n_a と、第1の認証情報 f_i (r , n_a , K_a) とを送信する(図6の通信301)。

【0193】次に、第2の局41は、ユーザ情報 I_a を用いて、ユーザ情報・アクセス回数・秘密情報格納部67から、第1の局11についてのアクセス回数 n'_a と秘密情報 K'_a とを見つけ出す。次にまず、第2の局41のアクセス回数認証手段65が、今回受信したアクセス回数 n_a について、 $n'_a + \epsilon > n_a > n'_a$ という不等式関係が成立するか否かを調べる(図6の処理312)。成立しなければ、第1の局11の正当性を認めない。

【0194】第1の局11の正当性を認めないこととなった場合は、第2の局41は認証動作を中止する。また第2の局41は、通信を終了させたり、第1の局11にエラーメッセージを出す等任意好適な処置をとる。

【0195】一方、上記の不等式関係が成立する場合は、ユーザ情報・アクセス回数・秘密情報格納部67に記憶してあるアクセス回数 n'_a を今回送信されてきたアクセス回数 n_a に変更する(図6の処理313)。そして、第2の局41の第3の認証情報生成手段51は、乱数 r と、アクセス回数 n'_a ($=n_a$) と、秘密情報 K'_a と、一方向性関数 f_i とにより、第2の認証情報 f_i (r , n'_a , K'_a) を計算する(図6の処理314)。

【0196】次に、第2の局41の認証手段59は、第1の認証情報 f_i (r , n_a , K_a) と第2の認証情報 f_i (r , n'_a , K'_a) とを比較する(図6の処理315)。この比較において両者が等しければ、第2の局41は、第1の局11の正当性を認め、通信許可信号"OK"と共有暗号鍵生成のための関数 g_j の番号 j とを、第1の局11に送信する(図6の通信302)。また、第2の局41の共有鍵生成手段53は、共有暗号鍵を $K_{12} = g_j(r, K'_a)$ のように生成する(図6の処理316)。

【0197】一方、通信許可信号"OK"を受信した第1の局11は、共有鍵生成手段23を用い共有暗号鍵を $K_{12} = g_j(r, K_a)$ のように生成する(図6の処理317)。

【0198】この第3の実施の形態によれば、ユーザ情報と第三者に知られていない秘密情報とを用いて、第2の局が第1の局の正当性を認証することができる。しかも、認証の際に用いた情報である乱数および秘密情報をそのまま用いて第1の局および第2の局の間に暗号鍵の共有を実現している。しかも、第1の局の認証処理と、第1の局および第2の局の間の共有暗号鍵の生成処理とを連続的に行なうことができる。

【0199】また送信されてきたアクセス回数が所定の不等式関係を満たすか否かにより、第1の局の正当性を判断することができる。そのため、正当でない通信者による攻撃を防止することができる。

【0200】また、第1の局が正当であることの認証は、第1の実施の形態と同様に行なうことができるの

で、安全性も確保できる。

【0201】またこの第2の実施の形態の方が、第1の実施の形態の場合に比べ、通信回数を少なくすることができる。

【0202】また、この第3の実施の形態では、第2の局41はアクセス回数を記憶するので、乱数履歴を記憶する場合に比べ第2の局41でのメモリを節約することができる。

【0203】4. 第4の実施の形態

次に、認証方法の第4の発明、暗号鍵共有方法の第2の発明、通信システムの第4および第12の発明それぞれの実施の形態を、併せて説明する。

【0204】4-1. 通信システムの構成説明

図7は第4の実施の形態の通信システムの構成を説明する図である。

【0205】上述の第1～第3の実施の形態では認証情報の生成を一方向性関数を用いて行なっていた。この第4の実施の形態では、認証情報を生成する際に、一方向性関数の代わりに、暗号化アルゴリズムを用いる。

【0206】この第4の実施の形態の第1の実施の形態との主な相違点は、第2の局41側に設けていた乱数生成手段49を省略し、第2の実施の形態と同じく第1の局11側に乱数生成手段29を設けた点と、第1の局11に、秘密情報を鍵として乱数およびユーザ情報を暗号化することにより認証情報を生成する認証情報生成手段33(暗号化部33ともいう)を設けた点と、

第1の局11に上記暗号化のためのアルゴリズムを複数記憶している記憶手段35(アルゴリズムEテーブル35ともいう)を設けた点と、第2の局に認証情報を復号する認証情報復号手段69(復号化部69ともいう)を設けた点と、第2の局41にアルゴリズムEテーブル35に対応するアルゴリズムEテーブル71を設けた点と、第2の実施の形態と同じく第2の局41にユーザ情報・乱数履歴・秘密情報格納部63を設けた点と、第2の局41に、第1の実施の形態で設けていた認証手段59の代わりに、乱数履歴およびユーザ情報に基づいて第1の局の正当性を認証する認証手段73を設けた点である。

【0207】ここで、アルゴリズムEテーブル35、71それぞれでは、格納された複数の暗号化アルゴリズムに、両局11、41で共通の番号を付してある。各アルゴリズムEテーブル35、71に対し同じ番号 q を入力することで、各アルゴリズムEテーブル35、71から、同じ暗号化アルゴリズム E_q を選択することができる。アルゴリズムEテーブル35は、送受信インタフェース17と認証情報生成手段としての暗号化部33とに接続してある。また、アルゴリズムEテーブル71は、送受信インタフェース45と認証情報復号化手段としての復号化部69とに接続してある。

【0208】なお、暗号化アルゴリズムの選択番号 q

は、例えば第1の局11の通信開始信号に応じて第1の局11または第2の局41が、例えば乱数を用いたり、予め用意されたプログラムに従い、生成する。第1の局11および第2の局41のいずれが番号 q を生成するかは、設計に応じ決めるのが良い。

【0209】ここで、暗号化アルゴリズムの具体例としては、たとえば、DES-CBCやMISTYやTriple DES-EDE-CBCなどを挙げることができる。その場合、アルゴリズムEテーブル35、71それぞれは、1. E_1 : DES-CBC 2. E_2 : MISTY 3. E_3 : Triple DES-EDE-CBC 4. ...のようにすることができる。

【0210】なお、アルゴリズムEテーブル35、71を用いることなく、第1の局11および第2の局41に共通な1つの暗号化アルゴリズムを、認証情報生成のための所定のアルゴリズムとする場合があっても良い。

【0211】また、認証情報生成手段33としての暗号化部33は、アルゴリズムEテーブル35から選択された暗号化アルゴリズム E_q を用い、乱数 r とユーザ情報 I_a とを、秘密情報 K_a を鍵として暗号化し、認証情報としての $E_q\{K_a, (r | E_q\{r, I_a\})\}$ を生成する手段である(詳細は後述する)。認証情報生成手段33の出力を送受信インターフェース17に接続してある。

【0212】また、認証情報復号手段69としての復号化部69は、第1の局11の認証情報生成手段33から送信されてきた認証情報としての $E_q\{K_a, (r | E_q\{r, I_a\})\}$ から、乱数 r とユーザ情報 I_a とを復号する手段である(詳細は後述する)。認証情報復号手段69の出力を認証手段73と接続してある。

【0213】また、認証手段73は、認証情報復号手段69で復号されたユーザ情報と第1の局から送信されてくるユーザ情報とを比較する比較部73aと、認証情報復号手段69で復号された乱数を乱数履歴と比較する比較部73bとで構成してある。この認証手段73は、2つの比較部73a、73bでそれぞれ比較結果が合格となった場合に、第1の局を正当と認証する手段である。

【0214】この第4の実施の形態の通信システムでは、乱数生成手段29、認証情報生成手段33、アルゴリズムEテーブル35、71、認証情報復号手段69、ユーザ情報・乱数履歴・秘密情報格納部63および認証手段73以外の構成は、第1の実施の形態と同じとしてある。

【0215】4-2. 動作の説明

次に、第3の実施の形態の通信システムの動作を説明する。これにより、認証方法および共有暗号鍵の生成方法の処理手順を説明する。この説明を図7に加えて図8を参照して行なう。図8は処理の流れを示した図である。

【0216】第1の局11の乱数生成手段29は、通信の際乱数 r を生成する。第1の局11の認証情報生成手

段33は、秘密情報 K_a を鍵に乱数 r とユーザ情報とを暗号化して認証情報を生成する。この場合は次のように暗号化をする。まず、乱数 r を鍵としてユーザ情報 I_a を暗号化して $E_q\{r, I_a\}$ という暗号文を得る。ただし E_q はアルゴリズムEテーブル35から選択された q 番目の暗号化アルゴリズムである。次に、秘密情報 K_a を鍵として乱数 r と上記の暗号文 $E_q\{r, I_a\}$ をさらに暗号化して、認証情報としての $E_q\{K_a, (r | E_q\{r, I_a\})\}$ を得る(図8の処理411)。ただし、記号“|”は連結を意味し、 $E\{K, X\}$ の表記は暗号鍵 K を用いて X を暗号化したものを意味する。

【0217】次に、第1の局11は、第2の局41に、ユーザ情報 I_a と、暗号化アルゴリズム選択番号 q と、認証情報としての $E_q\{K_a, (r | E_q\{r, I_a\})\}$ とを送信する(図8の通信401)。

【0218】認証情報としての $E_q\{K_a, (r | E_q\{r, I_a\})\}$ を受信した第2の局41は、ユーザ情報・乱数履歴・秘密情報格納部63から、ユーザ情報 I_a を用い第1の局についての秘密情報 K'_a (K_a)と乱数履歴とを見つけ出す。さらに第2の局41は認証情報復号化手段69を用いて、秘密情報 K'_a を鍵として、認証情報である暗号文 $E_q\{K_a, (r | E_q\{r, I_a\})\}$ を復号してすなわち解読して、乱数 r を得る。さらに、 r を鍵に $E_q\{r, I_a\}$ を復号してすなわち解読して、 I_a を得る(図8の処理412)。

【0219】次に、上記解読した r が乱数履歴に入っているか否かを認証手段73の比較部73aは調べる。また上記解読したユーザ情報と第1の局11から送信されてきたユーザ情報とを、比較部73bを用いて比較する(図8の処理413)。解読した乱数 r が乱数履歴に入っていた場合と、解読した I_a と受信した I_a が異なる場合との少なくとも一方が生じたら、認証手段73は第1の局11の正当性を認めない。

【0220】第1の局11の正当性を認めないこととなった場合は、第2の局41は認証動作を中止する。また第2の局41は、通信を終了させたり、第1の局11にエラーメッセージを出す等任意好適な処置をとる。

【0221】一方、解読した乱数 r が乱数履歴になく、かつ、解読したユーザ情報と送信されてきたユーザ情報とが等しい場合、認証手段73は、第1の局11の正当性を認める。第1の局11を正当と認めた場合(図8の処理414)、第2の局41は、通信許可信号“OK”と共有暗号鍵生成のための関数 g_j の番号 j とを、第1の局11に送信する(図8の通信402)。また、第2の局41の共有鍵生成手段53は、共有暗号鍵を $K_{12} = g_j(r)$ のように生成する(図8の処理415)。

【0222】一方、通信許可信号“OK”を受信した第1の局11は、共有鍵生成手段23を用い共有暗号鍵を

$K_{12} = g_j(r)$

のように生成する(図8の処理416)。

【0223】この第4の実施の形態によれば、ユーザ情報と第三者に知られていない秘密情報とを用いて、第2の局が第1の局の正当性を認証することができる。しかも、認証の際に用いた情報である乱数をそのまま用いて第1の局および第2の局の間に暗号鍵の共有を実現している。しかも、第1の局の認証処理と、第1の局および第2の局の間の共有暗号鍵の生成処理とを連続的に行なうことができる。

【0224】またユーザ認証を行うとき、復号した乱数を乱数履歴と比較している。乱数は通信ごとに異なる。第3者が通信情報を盗聴してこれを用いて第2の局を繰り返して攻撃しようとしてもこの通信情報から復号される乱数は乱数履歴に存在する。すると第2の局はこの通信情報を正当と認めない。そのため第3者の繰り返し攻撃を防止することができる。

【0225】5. 第5の実施の形態

次に、認証方法の第5の発明、暗号鍵共有方法の第3の発明、通信システムの第5および第13の発明それぞれの実施の形態を、併せて説明する。

【0226】5-1. 通信システムの構成説明

図9は第5の実施の形態の通信システムの構成を説明する図である。

【0227】この第5の実施の形態の通信システムは第4の実施の形態(図7)の通信システムを以下のように変更したものである。第1の局11に、乱数生成手段29の代わりに第1の乱数 r_1 および第2の乱数 r_2 を生成する乱数生成手段121を設ける。第1の局11に、認証情報生成手段33を設ける代わりに、第1の暗号文を生成する暗号文生成手段123と、暗号鍵生成手段125と、暗号鍵を用いて第1の暗号文をさらに暗号化して認証情報を生成する認証情報生成手段127とを設ける。第2の局41に、認証情報復号手段69と認証手段73とを設ける代わりに、復号鍵生成手段75と、復号鍵を用いて認証情報を復号する認証情報復号手段77と、復号されたユーザ情報に基づいて第1の局を認証する認証手段79と、第1の乱数 r_1 を認証する乱数認証手段81を設ける。

【0228】ここで、乱数生成手段121は、発生した乱数のうちの第2の乱数 r_2 を共有鍵生成手段23と、暗号文生成手段123と、認証情報生成手段127とに出力できるように、これら構成成分23、123、127と接続してある。さらに、第1の乱数 r_1 を暗号鍵生成手段125と送受信インタフェース17とに出力できるよう、これら構成成分125、17と接続してある。

【0229】暗号文生成手段123は、乱数生成手段121と、ユーザ情報格納部15と、アルゴリズムEテーブル35と、認証情報生成手段127とに接続してある。この暗号文生成手段123は、乱数 r_2 を鍵として

ユーザ情報1aを暗号化して第1の暗号文を生成し、これを認証情報生成手段127に出力する手段である(詳細は後述する)。暗号化のための暗号化アルゴリズムは、ここではアルゴリズムEテーブル35より入力される。

【0230】暗号鍵生成手段125は、乱数生成手段121と、秘密情報格納部13と、関数fテーブル19と、認証情報生成手段127とに接続してある。この暗号鍵生成手段125は、認証情報を生成するための鍵を、第1の乱数 r_1 と秘密情報 K_a と所定のアルゴリズムとにより生成し、これを認証情報生成手段127に出力する手段である(詳細は後述する)。ここでは、所定のアルゴリズムとして一方向性関数 f_i を用いる。一方向性関数 f_i は、関数fテーブル19より入力される。

【0231】認証情報生成手段127は、暗号鍵生成手段125で生成される暗号鍵を用いて、第2の乱数 r_2 と前記第1の暗号文とを暗号化して認証情報を生成する手段である(詳細は後述する)。この暗号化の際の暗号化アルゴリズムはアルゴリズムEテーブル35より入力される。認証情報生成手段127の出力は送受信インタフェース17に接続してある。

【0232】第2の局41の復号鍵生成手段75は、送信されてくる第1の乱数 r_1 と秘密情報 K'_a と所定のアルゴリズムとにより、認証情報を復号するための鍵(復号鍵)を生成する手段である(詳細は後述する)。ここでは、所定のアルゴリズムとして一方向性関数 f_i を用いる。一方向性関数 f_i は、関数fテーブル47より入力される。復号鍵生成手段75の出力は認証情報復号手段77に接続してある。

【0233】認証情報復号手段77は、復号鍵生成手段75で生成された復号鍵を用いて認証情報を復号する手段である(詳細は後述する)。復号化のためのアルゴリズムは、ここではアルゴリズムEテーブル71より入力される。認証情報復号手段77の出力は認証手段79に接続してある。

【0234】認証手段79は、この場合、復号されたユーザ情報と送信されてきたユーザ情報とを比較することにより、第1の局11の正当性を認証する手段である(詳細は後述する)。

【0235】第1の乱数を認証する手段81は、今回送信されてきた第1の乱数 r_1 が過去に送信されてきた乱数の履歴中に含まれるか否かを調べて、第1の局の正当性を認証する手段である(詳細は後述する)。

【0236】上記説明した手段以外は、第4の実施の形態と同じとしてある。

【0237】5-2. 動作の説明

次に、第5の実施の形態の通信システムの動作を説明する。これにより、認証方法および共有暗号鍵の生成方法の処理手順を説明する。この説明を図9に加えて図10を参照して行なう。図10は処理の流れを示した図であ

る。

【0238】第1の局11の乱数生成手段121は通信のごとに第1の乱数 r_1 および r_2 を生成する。第1の局11の暗号文生成手段123は、第2の乱数 r_2 を鍵として、かつ、暗号アルゴリズム E_q を使って、ユーザ情報 I_a を暗号化し、第1の暗号文ここでは $E_q\{r_2, I_a\}$ という暗号文を生成する。また第1の局11の暗号鍵生成手段125は、認証情報を生成するための暗号アルゴリズムの鍵としてここでは $f_i(r_1, K_a)$ を生成する。そして、認証情報生成手段127は、暗号鍵 $f_i(r_1, K_a)$ を用いて、かつ、暗号アルゴリズム E_q を使って、乱数 r_2 と第1の暗号文 $E_q\{r_2, I_a\}$ をさらに暗号化し、認証情報としての $E_q\{f_i(r_1, K_a), (r_2 | E_q\{r_2, I_a\})\}$ を生成する(図10の処理511)。

【0239】次に、第1の局11は、ユーザ情報 I_a 、第1の乱数 r_1 、方向性関数番号 i 、暗号化アルゴリズム番号 q および認証情報 $E_q\{f_i(r_1, K_a), (r_2 | E_q\{r_2, I_a\})\}$ を、第2の局41に送信する(図10の通信501)。

【0240】次に、第2の局41は、ユーザ情報 I_a を用いて、第1の局11についての乱数履歴と秘密情報 K'_a とを、ユーザ情報・乱数履歴情報・秘密情報格納部63から見つけ出す。次にまず、第2の局41の乱数認証手段81が、乱数履歴を調べて(図10の処理512)、もし受信した第1の乱数 r_1 が乱数履歴に入っているならば第1の局11の正当性を認めない。

【0241】乱数履歴を調べた結果、第1の局11の正当性を認めないこととなった場合は、第2の局41は認証動作を中止する。そして第2の局41は、通信を終了させたり、第1の局11にエラーメッセージを出す等任意好適な処置をとる。

【0242】一方、今回送信されてきた第1の乱数 r_1 が乱数履歴に含まれていなかった場合は、第2の局41の復号鍵生成手段75が復号鍵として $f_i(r_1, K'_a)$ を生成する。次に、第2の局41の認証情報復号手段77が、上記復号鍵 $f_i(r_1, K'_a)$ を用いて、認証情報 $E_q\{f_i(r_1, K_a), (r_2 | E_q\{r_2, I_a\})\}$ を復号すなわち解読して第2の乱数 r_2 を得る。さらに第2の局41の認証情報復号手段77が、上記解読した第2の乱数 r_2 を鍵として用い、第1の暗号文 $E_q\{r_2, I_a\}$ を復号すなわち解読してユーザ情報 I_a を得る(図10の処理513)。

【0243】また、第2の局41は今回送信されてきた第1の乱数 r_1 を、ユーザ情報・乱数履歴情報・秘密情報格納部63に、乱数履歴情報として追加する。

【0244】次に、第2の局41の認証手段79は、復号したユーザ情報と送信されてきたユーザ情報とを比較する(図10の処理514)。この比較において両者が等しければ(図10の処理515)、第2の局41は、

第1の局11の正当性を認め、通信許可信号"OK"と共有暗号鍵生成のための関数 g_j の番号 j とを、第1の局11に送信する(図10の通信202)。また、第2の局41の共有鍵生成手段53は、共有暗号鍵を $K_{12}=g_j(r_2)$

のように生成する(図10の処理516)。

【0245】一方、通信許可信号"OK"を受信した第1の局11は、共有鍵生成手段23を用い共有暗号鍵を $K_{12}=g_j(r_2)$

のように生成する(図10の処理517)。

【0246】この第5の実施の形態によれば、ユーザ情報と第三者に知られていない秘密情報とを用いて、第2の局が第1の局の正当性を認証することができる。しかも、認証の際に用いた情報である第2の乱数 r_2 をそのまま用いて第1の局および第2の局の間に暗号鍵の共有を実現している。しかも、第1の局の認証処理と、第1の局および第2の局の間の共有暗号鍵の生成処理とを連続的に行なうことができる。

【0247】また送信されてきた第1の乱数 r_1 が乱数履歴に含まれるか否かで、第1の局の正当性を判断することができる。そのため、正当でない通信者による繰り返し攻撃を防止することができる。

【0248】また、秘密情報をそのまま暗号鍵にしないで所定のアルゴリズムを用いて秘密情報を暗号鍵化するので、第4の実施の形態に比べ秘密保護能力が高いといえる。

【0249】また、2種類の乱数 r_1, r_2 を用いているのでその分、秘密保護能力が高いといえる。

【0250】6. 第6の実施の形態

次に、認証方法の第6の発明、暗号鍵共有方法の第2の発明、通信システムの第6および第12の発明それぞれの実施の形態を、併せて説明する。

【0251】6-1. 通信システムの構成説明

図11は第6の実施の形態の通信システムの構成を説明する図である。

【0252】この第6の実施の形態の第4の実施の形態(図7)との主な相違点は、第1の局11に、第3の実施の形態と同じくアクセス回数計数手段31を設けた点と、第1の局11に、認証情報生成手段33を設ける代わりに、ユーザ情報とアクセス回数とを暗号化する暗号化手段129と、暗号化手段129で暗号化された暗号をさらに暗号化し認証情報を生成する認証情報生成手段131とを設けた点と、第2の局41に、認証手段73の代わりに、復号されたユーザ情報およびアクセス回数に基づいて第1の局の正当性を認証する認証手段83を設けた点と、第2の局41に、ユーザ情報・乱数履歴情報・秘密情報格納部63の代わりに、第3の実施の形態と同じく、ユーザ情報・アクセス回数・秘密情報格納部67(ただし、この場合は復号されたアクセス回数を記憶する)を設けた点である。

【0253】ここで、暗号化手段129は、乱数 r を鍵としてユーザ情報 I_a とアクセス回数 n_a とを暗号化する手段である(詳細は後述する)。暗号化のための暗号化アルゴリズムは、ここではアルゴリズムEテーブル35より入力される。この暗号化手段129の出力は、認証情報生成手段131に接続してある。

【0254】認証情報生成手段131は、乱数と暗号化手段129で暗号化されたユーザ情報 I_a とアクセス回数 n_a とを、秘密情報 K_a を鍵としてさらに暗号化して認証情報を生成する手段である(詳細は後述する)。この暗号化の際の暗号化アルゴリズムはアルゴリズムEテーブル35より入力される。認証情報生成手段131の出力は送受信インタフェース17に接続してある。

【0255】第2の局41の認証手段83は、認証情報復号手段69で復号されたユーザ情報と第1の局から送信されてくるユーザ情報とを比較する比較部83aと、認証情報復号手段69で復号されたアクセス回数 n_a と格納部67に記憶してあるアクセス回数 n'_a との間に所定の不等式関係が成立するか否かを比較する比較部83bとで構成してある。所定の不等式とは例えば $n'_a + \epsilon > n_a > n'_a$ とすることができる。ここで ϵ は通信ミスなどを許容する数で例えば5程度である。この認証手段83は、2つの比較部83a、83bでそれぞれ比較結果が合格となった場合に、第1の局を正当と認証する。

【0256】上記以外の構成は第4の実施の形態と同じとしてある。

【0257】6-2. 動作の説明

次に、第6の実施の形態の通信システムの動作を説明する。これにより、認証方法および共有暗号鍵の生成方法の処理手順を説明する。この説明を図11に加えて図12を参照して行なう。図12は処理の流れを示した図である。

【0258】第1の局11の乱数生成手段29は、通信の際乱数 r を生成する。第1の局11のアクセス回数計数手段31は、計数値すなわちアクセス回数 n_a を1増加させ、 $n_a = n_a + 1$ とする。第1の局の暗号化手段129は、乱数 r を鍵としてかつ暗号アルゴリズム E_q を使って、ユーザ情報 I_a とアクセス回数 n_a とを暗号化しここでは $E_q \{r, I_a | n_a\}$ という暗号文を生成する。そして第1の局11の認証情報生成手段131は、秘密情報 K_a を鍵として、かつ、暗号アルゴリズム E_q を使って、乱数と上記の暗号文 $E_q \{r, I_a | n_a\}$ をさらに暗号化し、認証情報としての $E_q \{K_a, (r | E_q \{r, I_a | n_a\})\}$ を生成する(図12の処理611)。

【0259】次に、第1の局11は、ユーザ情報 I_a 、暗号化アルゴリズム番号 q および認証情報 $E_q \{K_a, (r | E_q \{r, I_a | n_a\})\}$ を、第2の局41に送信する(図12の通信601)。

【0260】次に、第2の局41は、ユーザ情報 I_a を

用いて、第1の局11についての秘密情報 K'_a と、いままでのアクセス回数 n'_a とを、ユーザ情報・アクセス回数・秘密情報格納部63から見つけ出す。

【0261】次に第2の局41は認証情報復号化手段69を用いて、秘密情報 K'_a を鍵として、認証情報である暗号文 $E_q \{K_a, (r | E_q \{r, I_a | n_a\})\}$ を復号してすなわち解読して、乱数 r を得る。さらに、 r を鍵に $E_q \{r, I_a | n_a\}$ を復号してすなわち解読して、 I_a と n_a とを得る(図12の処理612)。

【0262】次に、上記解読したユーザ情報と第1の局11から送信されてきたユーザ情報とを、認証手段83の比較部83aを用いて比較する。さらに、上記解読したアクセス回数 n_a が $n'_a + \epsilon > n_a > n'_a$ を満たすか否かを、比較部83bを用いて調べる(図12の処理613)。解読したアクセス回数 n_a が上記不等式を満たしていない場合と、解読した I_a と受信した I_a とが等しくない場合の少なくとも一方が生じたら、認証手段83は第1の局11の正当性を認めない。

【0263】第1の局11の正当性を認めないこととなった場合は、第2の局41は認証動作を中止する。また第2の局41は、通信を終了させたり、第1の局11にエラーメッセージを出す等任意好適な処置をとる。

【0264】一方、解読したアクセス回数 n_a が上記不等式を満たし、かつ、解読したユーザ情報と送信されてきたユーザ情報とが等しい場合、認証手段83は、第1の局11の正当性を認める。第1の局11を正当と認めた場合(図12の処理614)、第2の局41は、通信許可信号"OK"と共有暗号鍵生成のための関数 g_j の番号 j とを、第1の局11に送信する(図12の通信602)。しかも、格納部67に記憶してあるアクセス回数 n'_a を n_a に変更する(図12の処理615)。また、第2の局41の共有鍵生成手段53は、共有暗号鍵を

$$K_{12} = g_j(r)$$

のように生成する(図12の処理616)。

【0265】一方、通信許可信号"OK"を受信した第1の局11は、共有鍵生成手段23を用い共有暗号鍵を $K_{12} = g_j(r)$

のように生成する(図12の処理617)。

【0266】この第6の実施の形態によれば、ユーザ情報と第三者に知られていない秘密情報とを用いて、第2の局が第1の局の正当性を認証することができる。しかも、認証の際に用いた情報である乱数 r をそのまま用いて第1の局および第2の局の間に暗号鍵の共有を実現している。しかも、第1の局の認証処理と、第1の局および第2の局の間の共有暗号鍵の生成処理とを連続的に行なうことができる。

【0267】また第1の局の認証をおこなうとき、ユーザ情報とアクセス回数との両方を用い行なうので認証の信頼性を高めることができる。

【0268】さらにこの第6の実施の形態では通信ごとに値が変わるアクセス回数（認証情報から復号したアクセス回数）を認証している。もし通信情報を第3者が盗聴してそれを用いて第2の局を繰り返して攻撃した場合それはアクセス回数の部分がいつも同じ値の攻撃となるから、それは正当な通信とされない。そのため、第3者の繰り返して攻撃を防止することができる。

【0269】7. 第7の実施の形態

次に、認証方法の第7の発明、暗号鍵共有方法の第3の発明、通信システムの第7および第13の発明それぞれの実施の形態を、併せて説明する。

【0270】7-1. 通信システムの構成説明

図13は第7の実施の形態の通信システムの構成を説明する図である。

【0271】この第7の実施の形態の通信システムは、第5の実施の形態（図9）の通信システムを以下のように変更したシステムに相当する。：第1の局11に、第3の実施の形態と同じくアクセス回数計数手段31を設ける。：第5の実施の形態で用いていた暗号文生成手段123の代わりに、第2の乱数 r_2 を鍵としてユーザ情報 I_a とアクセス回数 n_a とを暗号化して第1の暗号文を生成する暗号文生成化手段133を設ける。：第5の実施の形態で第2の局41に設けていた乱数認証手段81を省略する。：第5の実施の形態で設けていた認証手段79の代わりに、第6の実施の形態と同じく復号されたユーザ情報およびアクセス回数に基づいて第1の局を認証する認証手段83を設ける。

【0272】それ以外の構成は第5の実施の形態と同じとしている。

【0273】7-2. 動作の説明

次に、第7の実施の形態の通信システムの動作を説明する。これにより、認証方法および共有暗号鍵の生成方法の処理手順を説明する。この説明を図13に加えて図14を参照して行なう。図14は処理の流れを示した図である。

【0274】第1の局11の乱数生成手段121は通信のごとに第1の乱数 r_1 および r_2 を生成する。第1の局11のアクセス回数計数手段31は、計数値すなわちアクセス回数 n_a を1増加させ、 $n_a = n_a + 1$ とする。第1の局11の暗号文生成手段133は、第2の乱数 r_2 を鍵として、かつ、暗号化アルゴリズム E_q を使って、ユーザ情報 I_a とアクセス回数 n_a とを暗号化して第1の暗号文ここでは $E_q \{r_2, I_a | n_a\}$ という暗号文を生成する。また第1の局11の暗号鍵生成手段125は、認証情報を生成するための暗号アルゴリズムの鍵としてここでは $f_i(r_1, K_a)$ を生成する。そして、認証情報生成手段127は、暗号鍵 $f_i(r_1, K_a)$ を用いて、かつ、暗号化アルゴリズム E_q を使って、乱数 r_2 と第1の暗号文 $E_q \{r_2, I_a | n_a\}$ をさらに暗号化し、認証情報としての $E_q \{f_i$

$(r_1, K_a), (r_2 | E_q \{r_2, I_a | n_a\})\}$ を生成する（図14の処理711）。

【0275】次に、第1の局11は、ユーザ情報 I_a 、第1の乱数 r_1 、一方向性関数番号 i 、暗号化アルゴリズム番号 q および認証情報 $E_q \{f_i(r_1, K_a), (r_2 | E_q \{r_2, I_a | n_a\})\}$ を、第2の局41に送信する（図14の通信701）。

【0276】次に、第2の局41は、ユーザ情報 I_a を用いて、第1の局11についての秘密情報 K'_a といままでのアクセス回数 n'_a とを、ユーザ情報・アクセス回数・秘密情報格納部67から見つけ出す。

【0277】次に第2の局41は認証情報復号化手段69を用いて、 $f_i(r_1, K'_a)$ を鍵として、認証情報である暗号文 $E_q \{f_i(r_1, K'_a), (r_2 | E_q \{r_2, I_a | n_a\})\}$ を復号してすなわち解読して、第2の乱数 r_2 を得る。さらに、第2の乱数 r_2 を鍵に $E_q \{r_2, I_a | n_a\}$ を復号してすなわち解読して、 I_a と n_a とを得る（図14の処理712）。

【0278】次に、上記解読したユーザ情報と第1の局11から送信されてきたユーザ情報とを、認証手段83の比較部83a用いて比較する。さらに、上記解読したアクセス回数 n_a が $n'_a + \epsilon > n_a > n'_a$ を満たすか否かを、比較部83bを用いて調べる（図14の処理713）。解読したアクセス回数 n_a が上記不等式を満たしていない場合と、解読した I_a と受信した I_a とが等しくない場合の少なくとも一方が生じたら、認証手段83は第1の局11の正当性を認めない。

【0279】第1の局11の正当性を認めないこととなった場合は、第2の局41は認証動作を中止する。また第2の局41は、通信を終了させたり、第1の局11にエラーメッセージを出す等任意好適な処置をとる。

【0280】一方、解読したアクセス回数 n_a が上記不等式を満たし、かつ、解読したユーザ情報と送信されてきたユーザ情報とが等しい場合、認証手段83は、第1の局11の正当性を認める。第1の局11を正当と認めた場合（図14の処理714）、第2の局41は、通信許可信号“OK”と共有暗号鍵生成のための関数 g_j の番号 j とを、第1の局11に送信する（図14の通信702）。しかも、格納部67に記憶してあるアクセス回数 n'_a を n_a に変更する（図14の処理715）。また、第2の局41の共有鍵生成手段53は、共有暗号鍵を

$$K_{12} = g_j(r_2)$$

のように生成する（図14の処理716）。

【0281】一方、通信許可信号“OK”を受信した第1の局11は、共有鍵生成手段23を用い共有暗号鍵を $K_{12} = g_j(r_2)$

のように生成する（図14の処理717）。

【0282】この第7の実施の形態によれば、ユーザ情報と第三者に知られていない秘密情報とを用いて、第2

の局が第1の局の正当性を認証することができる。しかも、認証の際に用いた情報である第2の乱数 r_2 をそのまま用いて第1の局および第2の局の間に暗号鍵の共有を実現している。しかも、第1の局の認証処理と、第1の局および第2の局の間の共有暗号鍵の生成処理とを連続的に行なうことができる。

【0283】また第1の局の認証をおこなうとき、ユーザ情報とアクセス回数との両方を用い行なうので認証の信頼性を高めることができる。

【0284】また、認証情報を生成するとき、乱数 r_2 を鍵として第1の暗号化をし、一方向性関数の値を鍵として第2の暗号化をしているので、第6の実施の形態に比べ機密保護性能が高まる。

【0285】さらにこの第7の実施の形態では通信ごとに値が変わるアクセス回数（認証情報から復号したアクセス回数）を認証している。もし通信情報を第3者が盗聴してそれを用いて第2の局を繰り返して攻撃した場合それはアクセス回数の部分がいつも同じ値の攻撃となるから、それは正当な通信とされない。そのため、第3者の繰り返し攻撃を防止することができる。

【0286】8. 第8の実施の形態

次に、認証方法の第8の発明、暗号鍵共有方法の第4の発明、通信システムの第8および第14の発明それぞれの実施の形態を、併せて説明する。図15は、この第8の実施の形態の通信システムの構成を説明する図である。

【0287】この第8の実施の形態は、通信を希望する第1の局11および第2の局41と、第2の局に代わって認証をする信頼できる第3の局151を含む通信システムにおいて、第1の局11の正当性を第2の局に代わって第3の局が認証しながら第1の局および第2の局の間に暗号鍵を共有するケースである。ただし前提条件として、第1の局11と第3の局151とが秘密情報を共有している。しかも、第2の局41と第3の局151との間の通信経路は安全であると仮定する。

【0288】この第8の実施の形態は、例えば、第1の局11が外界の多数の個人端末であり、第3の局151が企業内の多数の端末であり、第2の局41が第3の局のファイアウォールであるような通信システムに適用できる。そして、第2の局41の負荷を分散でき、また通信システムの秘密保護能力をより高めることが可能になる例である。以下、詳細に説明する。

【0289】8-1. 通信システムの構成説明

第1の局11は、秘密情報 K_a を格納する秘密情報格納部13と、ユーザ情報 I_a を格納するユーザ情報格納部15と、他局との送受信のための送受信インターフェース17と、乱数生成手段141と、認証情報生成手段143と、共有鍵生成手段23と、共有鍵格納部27とを具える。これら構成成分の接続関係は、第2の実施の形態（図3参照）での接続関係と同じ（関数 f テーブル、

関数 g テーブルを除いて同じ）としてある。

【0290】第2の局41は、他局との送受信のための送受信インターフェース45と、これに接続された共有鍵格納部91とを具える。なお第1の局11および第2の局41の間は、通信回線100aにより接続してある。

【0291】第3の局151は、正当な通信者ごとの少なくともユーザ情報 I_a および秘密情報 K'_a を格納するユーザ情報・秘密情報格納部153と、送受信インターフェース155と、認証手段157と、共有鍵生成手段159とを具える。第2の局41および第3の局151の間は、通信回線100bにより接続してある。

【0292】ユーザ情報・秘密情報格納部153は、送受信インターフェース155と、認証手段157と、共有鍵生成手段159とに接続してある。認証手段157は送受信インターフェース155に接続してある。共有鍵生成手段159は送受信インターフェース155に接続してある。

【0293】なお、ユーザ情報・秘密情報格納部153について少なくともユーザ情報 I_a および秘密情報 K'_a を格納すると述べたのは、認証方法次第では、乱数履歴、アクセス回数、復号した乱数履歴または復号したアクセス回数を記憶する場合があっても良いという意味である。また、秘密情報 K_a 、 K'_a は同じものであるが、第1、第3のどちらの局側の秘密情報かを区別するために、 K_a 、 K'_a と称している。

【0294】ここで、第1の局11の認証情報生成手段143は、乱数生成手段141で発生される乱数と秘密情報格納部13に格納してある秘密情報 K_a とを用い認証情報を生成するものであれば、任意好適なものでできる。例えば、一方向性関数 f_i を用いたり、または、暗号化アルゴリズムを用いて認証情報を生成することができる。具体的には、第1の実施の形態で説明した手段21、第4の実施の形態で説明した手段33、

第5の実施の形態で説明した手段123、125および127を含む手段、第6の実施の形態で説明した手段129および131を含む手段、または、第7の実施の形態で説明した手段125、127および133を含む手段、により認証情報生成手段を構成することができる。もちろん、認証情報生成手段143を上記のいずれかで構成する場合は、それについて説明した第1～第7の実施の形態のいずれかの教示に従い、第1の局内の構成を変更する。

【0295】また乱数生成手段141は例えば通信ごとに乱数 r を発生する手段である。この乱数生成手段141は、認証情報生成手段143と、共有鍵生成手段23と、送受信インターフェース17とに接続してある。なお、乱数生成手段141は、認証情報生成手段143の構成の仕方によっては、第1の乱数 r_1 および第2の乱数 r_2 を生成する手段としても良い。

【0296】また第3の局151の認証手段157は、第1の局11からの認証情報を秘密情報 K'_a を用い認証する手段である。この認証手段157の構成は、第1の局11の認証情報生成手段143をどのように構成したかに応じ決める。認証情報生成手段143を上記の(1)のいずれかで構成する場合は、それに対応して、(1)第1の実施の形態で説明した手段51および59を含む手段、(2)第4の実施の形態で説明した手段69および73を含む手段、(3)第5の実施の形態で説明した手段75、77および79を含む手段、(4)第6の実施の形態で説明した手段69および83を含む手段、または、(5)第7の実施の形態で説明した手段75、77および83を含む手段、により認証手段157を構成することができる。もちろん、認証手段143を上記の(1)～(5)のいずれかで構成する場合は、それについて説明した第1～第7の実施の形態のいずれかの教示に従い第3の局内の構成を変更する。

【0297】また、第1の局11の共有鍵生成手段23および共有鍵格納部27は、それぞれ、第1～第7の実施の形態にて説明した手段23、27で構成できる。第3の局151の共有鍵生成手段159は、認証手段157が第1の局を正当と判断したときに、認証に用いた情報のうちの1または複数を用い、共有暗号鍵を生成する手段である。また、第2の局41の共有鍵格納部91は、第3の局で生成されそこから送信されてくる共有鍵を格納する手段である。

【0298】8-2. 動作の説明

次に、第8の実施の形態の通信システムの動作を説明する。これにより、認証方法および共有暗号鍵の生成方法の処理手順を説明する。この説明を図15に加えて図16を参照して行なう。図16は処理の流れを示した図である。

【0299】第1の局11の乱数生成手段141は通信に当たり乱数 r を発生する。第1の局の認証情報生成手段143は乱数 r と秘密情報 K_a とを用いて認証情報 A_a を生成する(図16の処理811)。この認証情報 A_a は、すでに説明したように、認証情報生成手段143の構成次第で任意のものとなる。

【0300】次に、第1の局11は、乱数 r とユーザ情報 I_a と認証情報 A_a とを、第2の局41に送信する(図16の通信801)。

【0301】第2の局41は、秘密情報と認証機能をもっていないので、第1の局11から送られた乱数 r とユーザ情報 I_a と認証情報 A_a とを第3の局151に転送する(図16の通信802)。

【0302】第3の局151は、第2の局41から転送されてきたユーザ情報 I_a を用いユーザ情報・秘密情報格納部153から第1の局11についての秘密情報 K'_a を見つけ出す。そして、第2の局41から転送されてきた認証情報 A_a を、第3の局151は秘密情報 K'_a を用いて

認証する(図16の処理813)。この認証は例えば次のように行うことができる。認証情報 A_a は、乱数 r と秘密情報 K_a とを用いたものである。第3の局151は認証情報 A_a から秘密情報 K'_a を用い乱数 r を得ることができる。また、別途に乱数 r は送信されている。したがって、認証情報から得た乱数と送信されてきた乱数とを比較することで、第1の局の正当性を認証することができる。もちろん、秘密情報 K'_a を用いて認証する具体的な方法は、すでに説明したが、認証情報生成143や認証手段157それぞれをどのように構成するかで変更することができる。

【0303】上記の認証において第1の局が正当とされた場合(図16の処理814)、第3の局151の共有鍵生成手段159は共有暗号鍵 K_{12} を生成する(図16の処理815)。また、第3の局151は、生成した共有暗号鍵 K_{12} と、通信許可信号"OK"とを第2の局41に送信する(図16通信803)。なお共有暗号鍵 K_{12} の生成アルゴリズムは、第1および第3の局の間で決めた任意のアルゴリズムとできる。例えば乱数および秘密情報 K_a を使って $g_j(r, K_a)$ のように作成することができる。もちろん、関数 g テーブルを用いるような方法でも良い。

【0304】共有暗号鍵 K_{12} と通信許可信号"OK"とを受信した第2の局41は、共有暗号鍵 K_{12} を共有鍵格納部91に格納し、また、通信許可信号"OK"を第1の局11に送信する(図16の通信804)。

【0305】通信許可信号"OK"を受信した。第1の局11は共有暗号鍵 K_{12} を生成し(図16の処理816)、これを共有鍵格納部27に格納する。

【0306】この第8の実施の形態によれば、秘密情報を共有しかつ認証情報と共有鍵の生成手段とを持つ第1の局および第3の局の間に、秘密情報を持たない第2の局が介在しても、第1の局の認証を実現することができ、然も第1の局および第2の局の間での暗号鍵の共有を実現することができる。また信頼できる第3の局が第2の局に代わって第1の局の正当性を認証するので、第2の局の負荷を減らすことができる。特に、第1の局と第3の局それぞれが多数の端末からなるグループの場合、第2の局の負荷分散が実現される。

【0307】またこの第8の実施の形態の場合も、認証の際に用いた情報を用いて第1の局および第2の局の間に暗号鍵の共有を実現している。しかも、第1の局の認証処理と、第1の局および第2の局の間の共有暗号鍵の生成処理とを連続的行なうことができる。

【0308】9. 第9の実施の形態

次に、認証方法の第9の発明、暗号鍵共有方法の第4の発明、通信システムの第9および第14の発明それぞれの実施の形態を、併せて説明する。

【0309】図17は第9の実施の形態の通信システムの構成を説明する図である。第8の実施の形態では乱数

生成手段を第 1 の局 1 1 内に設ける例を説明した。これに対し、この第 9 の実施の形態では、第 2 の局 4 1 に乱数生成手段 9 3 を設けた例である。それ以外の構成は第 8 の実施の形態と同様としてある。

【0310】第 2 の局 4 1 に設けた乱数生成手段 9 3 は、送受信インタフェース 4 5 に接続している。しかも、乱数生成手段 9 3 が発生した乱数は、第 1 の局 1 1 の認証情報生成手段 1 4 3 および共有鍵生成手段 2 3 と、第 3 の局 1 5 1 の認証手段 1 5 7 および共有鍵生成手段 1 5 9 に送信される構成としてある。なお、認証情報生成手段 1 4 3 および認証手段 1 5 7 の構成が、第 5

の実施の形態などのように乱数 r_1 および乱数 r_2 を用いる場合は、乱数生成手段 9 3 も乱数 r_1 および乱数 r_2 を発生する構成とする。

【0311】次に、第 9 の実施の形態の通信システムの動作について、図 17 に加えて図 18 を参照して説明する。図 18 は処理の流れを示した図である。

【0312】第 1 の局 1 1 は第 2 の局 4 1 にユーザ情報 I_a を送信する（図 18 の通信 9 0 1）。

【0313】第 2 の局 4 1 はユーザ情報 I_a を受信すると乱数生成手段 9 3 を用いて乱数 r を発生しこれを第 1

の局 1 1 に返信する（図 18 の通信 9 0 2）。

【0314】第 1 の局 1 1 の認証情報生成手段 1 4 3 は、乱数 r と秘密情報 K_a とを用い認証情報 A_a を生成し（図 18 の処理 9 1 1）、これを第 2 の局 4 1 に送信する（図 18 の通信 9 0 3）認証情報 A_a を受信した第 2 の局 4 1 は、認証情報 A_a と乱数 r とユーザ情報 I_a とを、第 3 の局 1 5 1 に送信する（図 18 の通信 9 0 4）。

【0315】第 3 の局 1 5 1 は、第 2 の局 4 1 から送信されきたユーザ情報 I_a を用いユーザ情報・秘密情報格納部 1 5 3 から第 1 の局 1 1 についての秘密情報 K'_a を見つけ出す。そして、第 2 の局 4 1 から転送されきた認証情報 A_a を、第 3 の局 1 5 1 は秘密情報 K'_a を用いて認証する（図 18 の処理 9 1 2）。この認証は例えば第 8 の実施の形態で説明したように行うことができる。

【0316】上記の認証において第 1 の局が正当とされた場合（図 18 の処理 9 1 3）、第 3 の局 1 5 1 の共有鍵生成手段 1 5 9 は共有暗号鍵 K_{12} を生成する（図 18 の処理 9 1 4）。また、第 3 の局 1 5 1 は、生成した共有暗号鍵 K_{12} と、通信許可信号“OK”とを第 2 の局 4

1 に送信する（図 18 通信 9 0 5）。

【0317】共有暗号鍵 K_{12} と通信許可信号“OK”とを受信した第 2 の局 4 1 は、共有暗号鍵 K_{12} を共有鍵格納部 9 1 に格納し、また、通信許可信号“OK”を第 1 の局 1 1 に送信する（図 18 の通信 9 0 6）。

【0318】通信許可信号“OK”を受信した第 1 の局 1 1 は、共有暗号鍵生成手段 2 3 を用い共有暗号鍵 K_{12} を生成し（図 18 の処理 9 1 5）、これを共有鍵格納部 2 7 に格納する。

【0319】この第 9 の実施の形態によれば、秘密情報を共有しかつ認証情報と共有鍵の生成手段とを持つ第 1 の局および第 3 の局の間に、秘密情報を持たない第 2 の局が介在しても、第 1 の局の認証を実現することができる。然も第 1 の局および第 2 の局の間での暗号鍵の共有を実現することができる。また信頼できる第 3 の局が第 2 の局に代わって第 1 の局の正当性を認証するので、第 2 の局の負荷を減らすことができる。特に、第 1 の局と第 3 の局それぞれが多数の端末からなるグループの場合、第 2 の局の負荷分散が実現される。

【0320】またこの第 9 の実施の形態の場合も、認証の際に用いた情報を用いて第 1 の局および第 2 の局の間に暗号鍵の共有を実現している。しかも、第 1 の局の認証処理と、第 1 の局および第 2 の局の間の共有暗号鍵の生成処理とを連続的に行うことができる。

【0321】またこの第 9 の実施の形態の場合は乱数を第 2 の局が発生するので、第 1 の局自体が自ら適正な乱数を得ることができない。そのためもし第三者が第 2 の局に繰り返し攻撃を行おうとしても、それを防止することができる。

【0322】10. 第 10 の実施の形態

次に、認証方法の第 10 の発明、暗号鍵共有方法の第 5 の発明、通信システムの第 10 および第 15 の発明それぞれの実施の形態を、併せて説明する。

【0323】図 19 は、この第 10 の実施の形態の通信システムの構成を説明する図である。

【0324】この第 10 の実施の形態は、通信を希望する第 1 の局 1 1 および第 2 の局 4 1 と、これら局 1 1、4 1 間に介在する中間局 1 6 1 とを含む通信システムにおいて、第 1 の局 1 1 の正当性を第 2 の局が認証しながら第 1 の局および第 2 の局の間で暗号鍵を共有するケースである。ただし前提条件として、第 1 の局 1 1 と第 3 の局 1 5 1 とが秘密情報を共有している。しかも、中間局 1 6 1 が乱数生成手段を具えている。しかも、中間局 1 6 1 と第 1 の局 1 1 との間の通信経路、中間局 1 6 1 と第 2 の局 4 1 との間の通信経路が安全か否かは問わない。

【0325】10-1. 通信システムの構成説明

第 1 の局 1 1 は、乱数生成手段を省略した点を除いて第 8 の実施の形態の場合の第 1 の局と同じ構成としてある。

【0326】第 2 の局 4 1 は、他局との送受信のための送受信インタフェース 4 5 と、正当な通信者ごとの少なくともユーザ情報 I_a および秘密情報 K'_a を格納するユーザ情報・秘密情報格納部 9 5 と、認証手段 9 7 と、共有鍵生成手段 9 9 と、共有鍵格納部 5 7 とを具える。ユーザ情報・秘密情報格納部 9 5 は、送受信インタフェース 4 5 と、認証手段 9 7 と、共有鍵生成手段 9 9 とに接続してある。認証手段 9 7 は送受信インタフェース 4

フェース45に接続してある。

【0327】なお、ユーザ情報・秘密情報格納部95について少なくともユーザ情報 I_a および秘密情報 K'_a を格納すると述べたのは、認証方法次第では、乱数履歴、アクセス回数、復号した乱数履歴または複合したアクセス回数を記憶する場合があっても良いという意味である。

【0328】認証手段97は、第1の局11から中間局161を介し送信されてくる認証情報 A_a を、格納部95に格納してある秘密情報 K'_a を用い認証する手段である。この認証手段97は、第1の局11の認証情報生成手段143の構成に応じた構成とする。

【0329】中間局161は、他局との送受信のための送受信インターフェース163と、これに接続された乱数生成手段165とを具える。乱数生成手段165が発生した乱数は、第1の局11の認証情報生成手段143および共有鍵生成手段23と、第2の局41の認証手段97および共有鍵生成手段99に送信できる構成としてある。

【0330】第1の局11と中間局161とは通信回線101cにより接続してあり、第2の局41と中間局161とは通信回線101dにより接続してある。

【0331】10-2. 動作の説明

次に、第10の実施の形態の通信システムの動作について、図19に加えて図20を参照して説明する。図20は処理の流れを示した図である。

【0332】第1の局11は中間局161にユーザ情報 I_a を送信する(図20の通信1001)。

【0333】中間局161はユーザ情報 I_a を受信すると乱数生成手段165を用いて乱数 r を発生しこれを第1の局11に返信する(図20の通信1002)。

【0334】第1の局11の認証情報生成手段143は、乱数 r と秘密情報 K_a とを用い認証情報 A_a を生成し(図20の処理911)、これを中間局161に送信する(図20の通信1003)。

認証情報 A_a を受信した中間局161、認証情報 A_a と乱数 r とユーザ情報 I_a とを、第2の局41に送信する(図20の通信1004)。

【0335】第2の局41は、中間局161から送信されてきたユーザ情報 I_a を用いユーザ情報・秘密情報格納部95から第1の局11についての秘密情報 K'_a を見つけ出す。そして、中間局161から転送されてきた認証情報 A_a を、第2の局41は、秘密情報 K'_a を用いて認証する(図20の処理1012)。この認証は例えば第8の実施の形態で説明したように行うことができる。

【0336】上記の認証において第1の局が正当とされた場合(図20の処理1013)、第2の局41の共有鍵生成手段99は共有暗号鍵 K_{12} を生成する(図20の処理1014)。また、第2の局41は、通信許可信号"OK"を中間局161に送信する(図20通信10

05)。

【0337】通信許可信号"OK"を受信した中間局161は、通信許可信号"OK"を第1の局11に送信する(図20の通信1006)。

【0338】通信許可信号"OK"を受信した第1の局11は、共有暗号鍵生成手段23を用い共有暗号鍵 K_{12} を生成し(図20の処理1015)、これを共有鍵格納部27に格納する。

【0339】この第10の実施の形態によれば、秘密情報を共有しかつ認証情報と共有鍵の生成手段とを持つ第1の局および第2の局の間に、秘密情報を持たない中間局が介在しても、第1の局の認証を実現することができ、然も第1の局および第2の局の間での暗号鍵の共有を実現することができる。

【0340】またこの第10の実施の形態の場合も、認証の際に用いた情報を用いて第1の局および第2の局の間に暗号鍵の共有を実現している。しかも、第1の局の認証処理と、第1の局および第2の局の間の共有暗号鍵の生成処理とを連続的に行なうことができる。

【0341】また中間局に乱数発生の仕事を受け持たせたので、第1および第2の局の負荷を軽減することができる。

【0342】上述においてこの出願の各発明の実施の形態について説明した。しかしこれら発明は、上述の実施の形態に何ら限定されるものではなく、多くの変形または変更を行うことができる。

【0343】たとえば、一方向性関数 $f_i(x, y)$ の変数利用形態として、 $f_i(x|y)$ 、 $f_i(x \text{ AND } y)$ 、 $f_i(x \text{ XOR } y)$ などの形を使用しても良い。

【0344】が使える。ただし、 $x|y$ は連結を意味する。

【0345】また、第4～第7の各実施の形態では、共有暗号鍵を生成するとき、乱数 r (あるいは r_2)が暗号文で送られているため秘密情報を使わずに $g_j(r)$ (あるいは $g_j(r_2)$)を共有暗号鍵としているが、共有暗号鍵を生成するとき秘密情報 K_a (K'_a)を変数に加えれば安全性がさらに高められる。

【0346】また、第4の実施の形態では暗号アルゴリズムの暗号化鍵として秘密情報 K_a を使い、また、第5～第7の各実施の形態では暗号アルゴリズムの暗号化鍵として $f_i(r_1, K_a)$ を使っている。しかし、暗号アルゴリズムによっては鍵の長さが合わないかも知れない。例えば、一方向性関数がMD5の場合には、鍵である $f_i(r_1, K_a)$ が128ビットとなる。このとき暗号化アルゴリズムとしてDES-CBCを用いたとすると、この鍵は長すぎる。そのような場合の対応方法として、鍵が必要以上に長い場合は上位ビットを切り捨てるか、短い場合は上位ビットに0を入れるなどの方法がある。 $E_q\{r_2, I_a\}$ 、 $E_q\{r_2, I_a|n_a\}$ の中の乱数についても、それが暗号化アルゴリズム E_q

に対し長かったり短かったりした場合は上記と同じ扱いとすることができる。

【0347】

【発明の効果】上述した説明から明らかなように、この出願の認証方法の各発明によれば、ユーザ情報と秘密情報とを用いて第1の局を第2の局（または第3の局）が認証することができる新規な方法が実現できる。このため、暗号通信に当たって正当な通信相手を確認することができる。

【0348】また特に、 α ：第1の局から送信されてきた乱数が乱数履歴に含まれるか否かを調べる処理を含む発明、 β ：第1の局によるアクセス回数が不等式関係を満たすか否かを調べる処理を含む発明、 γ ：第1の局から送信された認証情報から復号した乱数が乱数履歴に含まれるか否かを調べる処理を含む発明、 δ ：第1の局から送信された認証情報から復号したアクセス回数が不等式関係を満たすか否かを調べる処理を含む発明それぞれは、1度通信で用いた情報を再度通信に利用することを排除することができる。そのため、第3者が通信情報を盗聴してこれを利用して通信システムを攻撃しようとしても、それを防止することができる。

【0349】またこの出願の暗号鍵共有方法の各発明によれば、認証方法において用いた情報の1または複数をそのまま利用して共有暗号鍵を生成でき、しかも、認証方法の生成処理に連続して共有暗号鍵を生成することができる。認証処理が終了後に共有暗号鍵生成のための通信を別途に行なう場合、この別途の通信の際に盗聴を受ける等の危険があるが、この発明の暗号鍵共有方法ではそれを防止することができる。

【0350】また、この出願の通信システムの各発明によれば、対応する認証方法の発明や対応する共有暗号鍵の生成方法の発明を容易に実施することができる。

【図面の簡単な説明】

【図1】第1の実施の形態の通信システムの構成説明図である。

【図2】第1の実施の形態の通信システムの動作説明図である。

【図3】第2の実施の形態の通信システムの構成説明図である。

【図4】第2の実施の形態の通信システムの動作説明図である。

【図5】第3の実施の形態の通信システムの構成説明図である。

【図6】第3の実施の形態の通信システムの動作説明図である。

【図7】第4の実施の形態の通信システムの構成説明図である。

【図8】第4の実施の形態の通信システムの動作説明図である。

【図9】第5の実施の形態の通信システムの構成説明図

である。

【図10】第5の実施の形態の通信システムの動作説明図である。

【図11】第6の実施の形態の通信システムの構成説明図である。

【図12】第6の実施の形態の通信システムの動作説明図である。

【図13】第7の実施の形態の通信システムの構成説明図である。

10 【図14】第7の実施の形態の通信システムの動作説明図である。

【図15】第8の実施の形態の通信システムの構成説明図である。

【図16】第8の実施の形態の通信システムの動作説明図である。

【図17】第9の実施の形態の通信システムの構成説明図である。

【図18】第9の実施の形態の通信システムの動作説明図である。

20 【図19】第10の実施の形態の通信システムの構成説明図である。

【図20】第10の実施の形態の通信システムの動作説明図である。

【符号の説明】

11：第1の局

13：秘密情報格納部

15：ユーザ情報格納部

19、47：関数fテーブル（所定のアルゴリズムを複数記憶する手段）

30 21：第1の認証情報生成手段

23：共有鍵生成手段

25、55：関数gテーブル（暗号鍵生成アルゴリズムを複数記憶する手段）

29：乱数生成手段

31：アクセス回数計数手段

33：認証情報生成手段（暗号化部）

35、71：アルゴリズムEテーブル（暗号化アルゴリズムを複数記憶する手段）

41：第2の局

40 43：ユーザ情報・秘密情報格納部

49：乱数生成手段

51：第2の認証情報生成手段

53：共有鍵生成手段

61：乱数認証手段

63：ユーザ情報・乱数履歴情報・秘密情報格納部

65：アクセス回数認証手段

67：ユーザ情報・アクセス回数・秘密情報格納部

69：認証情報復号化手段

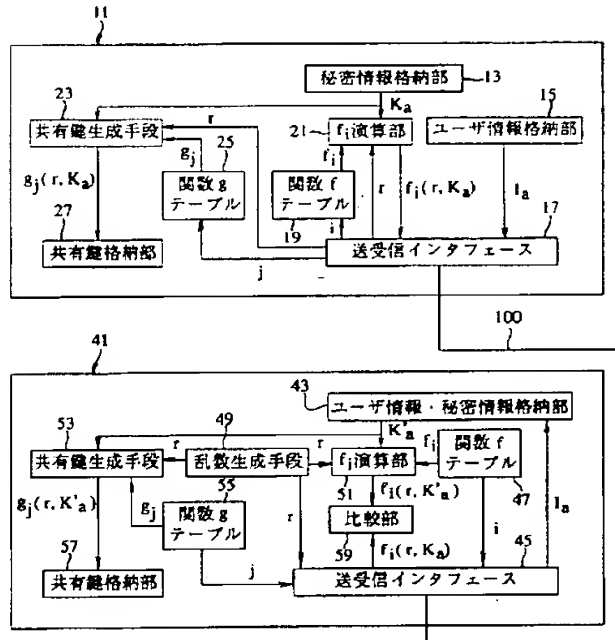
73：認証手段

50 75：復号鍵生成手段

77: 認証情報復号化手段
 79: 認証手段
 81: 第1の乱数を認証する手段
 83: 認証手段
 100、100a~100d: 通信回線
 121: 乱数生成手段
 123: 暗号文生成手段

125: 暗号鍵生成手段
 127: 認証情報生成手段
 129: 暗号化手段
 131: 認証情報生成手段
 133: 暗号文生成手段
 151: 第3の局
 161: 中間局

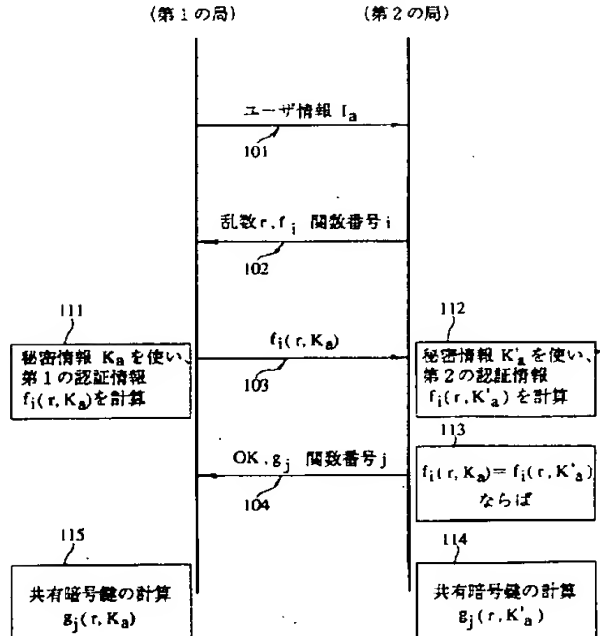
【図1】



11: 第1の局
 21: 第1の認証情報生成手段 (f_i 演算部)
 51: 第2の認証情報生成手段 (f_i 演算部)
 59: 認証手段 (比較部)
 1a: ユーザ情報
 Ka, Ka': 秘密情報
 41: 第2の局
 100: 通信回線
 r: 乱数

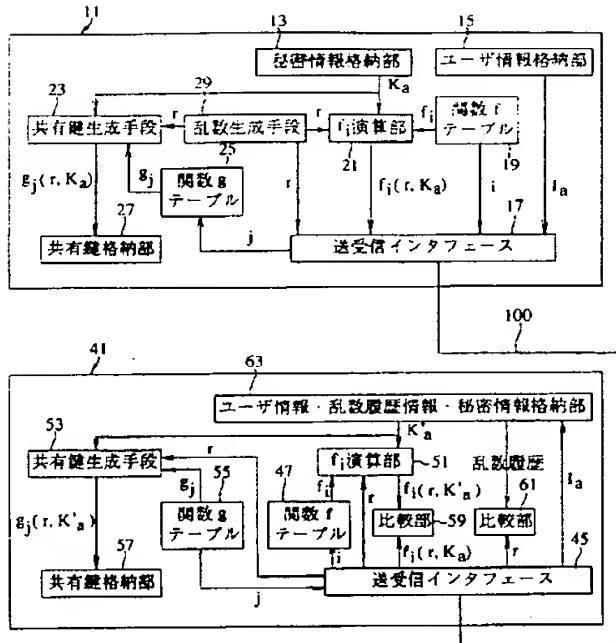
第1の実施の形態の通信システムの構成説明図

【図2】



第1の実施の形態の通信システムの動作説明図

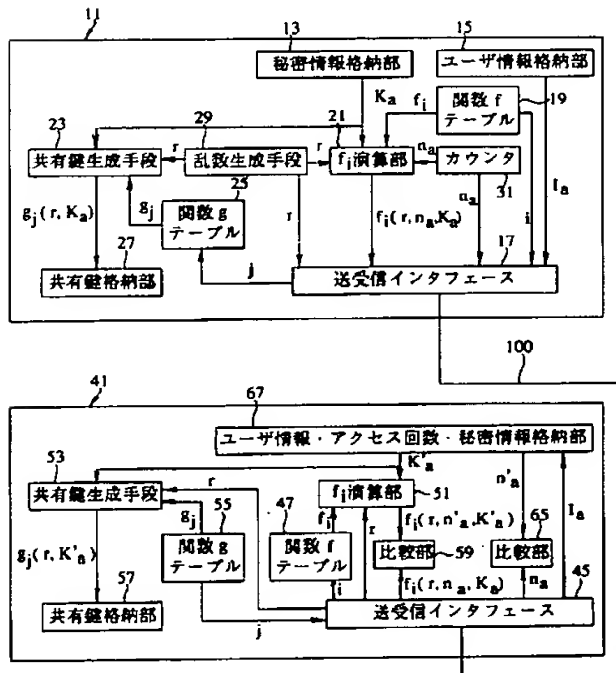
【図3】



61: 乱数認証手段 (比較部)

第2の実施の形態の通信システムの構成説明図

【図5】

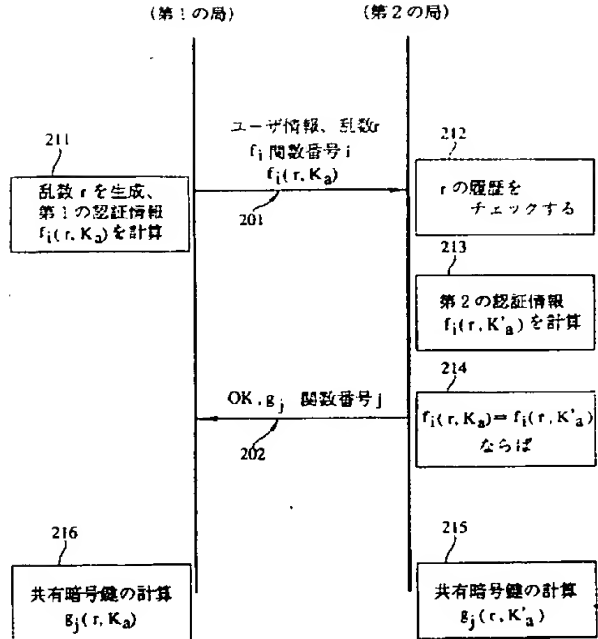


31: アクセス回数計数手段 (カウンタ)

65: アクセス回数認証手段 (比較部)

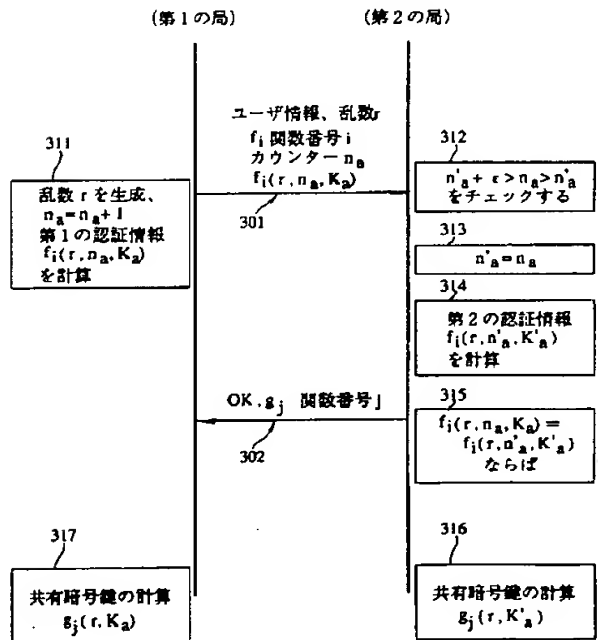
第3の実施の形態の通信システムの構成説明図

【図4】



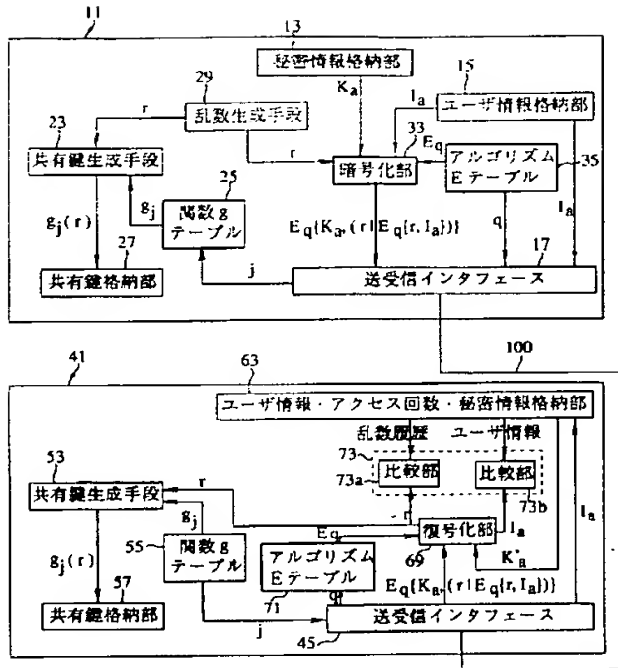
第2の実施の形態の通信システムの動作説明図

【図6】



第3の実施の形態の通信システムの動作説明図

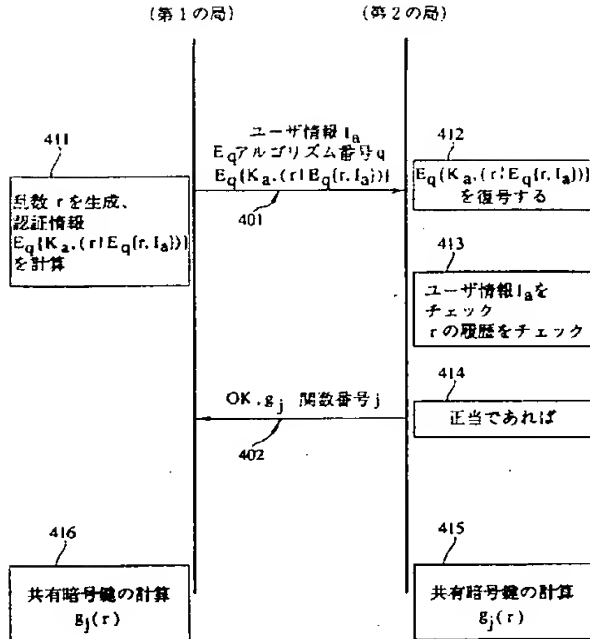
【図 7】



33: 認証情報生成手段 (暗号化部)
 69: 認証情報復号化手段 (復号化部)
 73: 認証手段

第 4 の実施の形態の通信システムの構成説明図

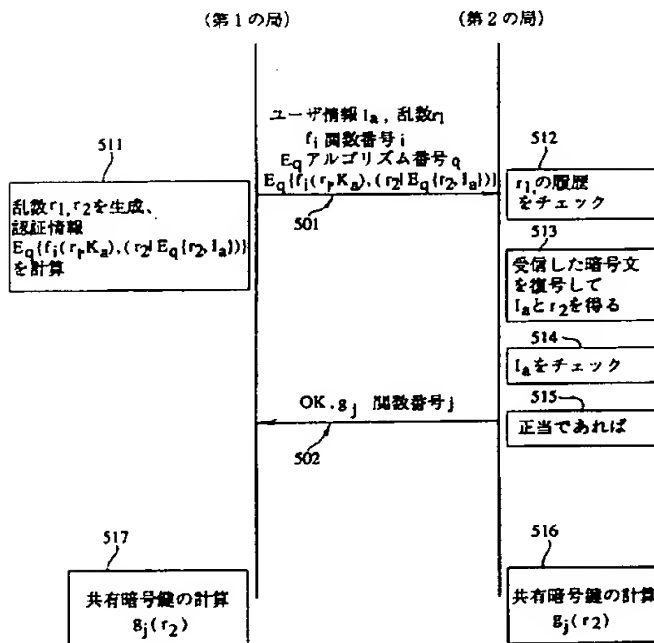
【図 8】



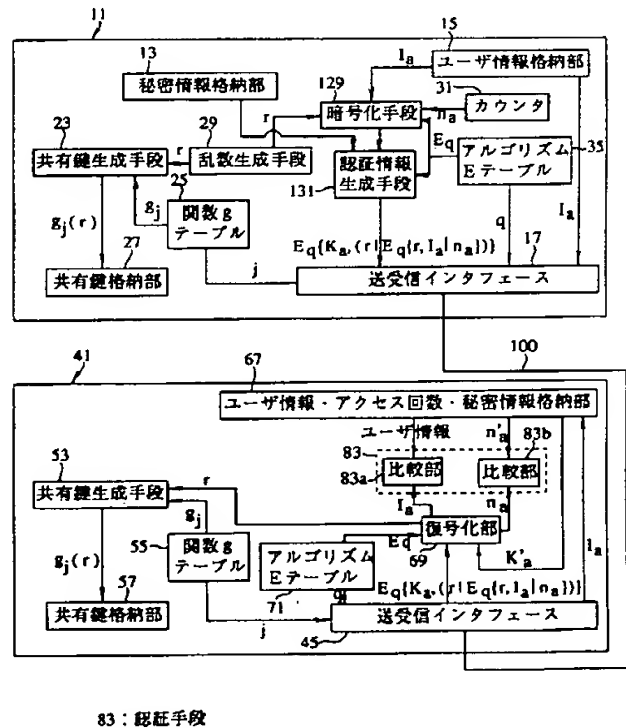
第 4 の実施の形態の通信システムの動作説明図

【図 11】

【図 10】



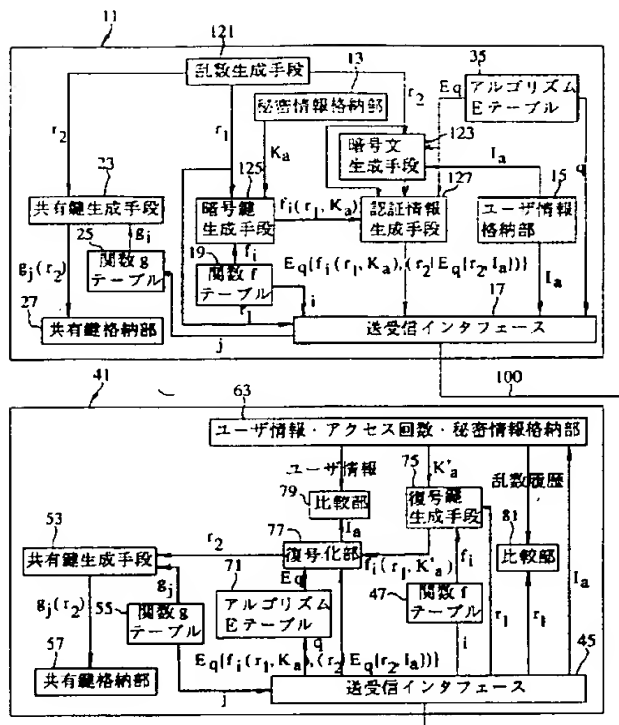
第 5 の実施の形態の通信システムの動作説明図



83: 認証手段

第 6 の実施の形態の通信システムの構成説明図

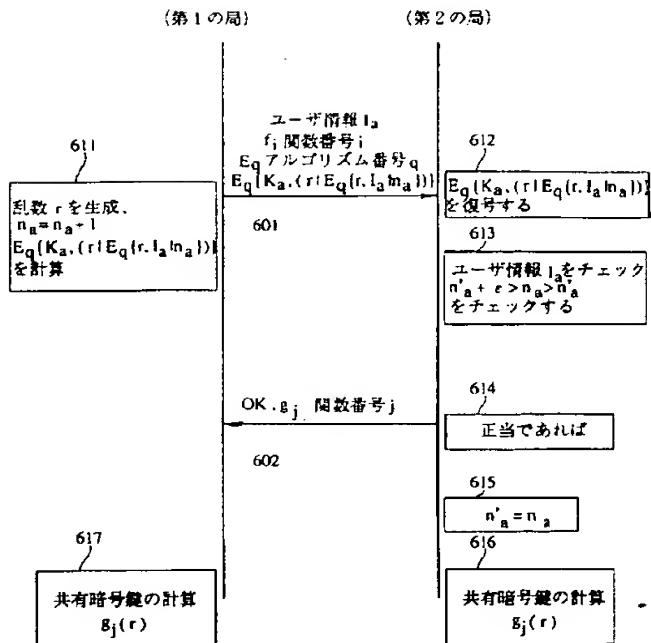
【図9】



77: 認証情報復号化手段 (復号化部)
 79: 認証手段 (比較部)
 81: 第1の乱数を認証する手段 (比較部)

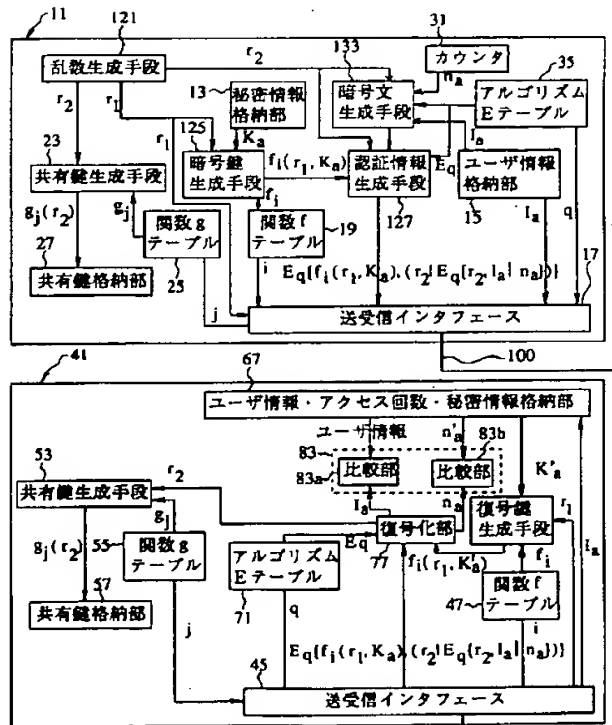
第5の実施の形態の通信システムの構成説明図

【図12】



第6の実施の形態の通信システムの動作説明図

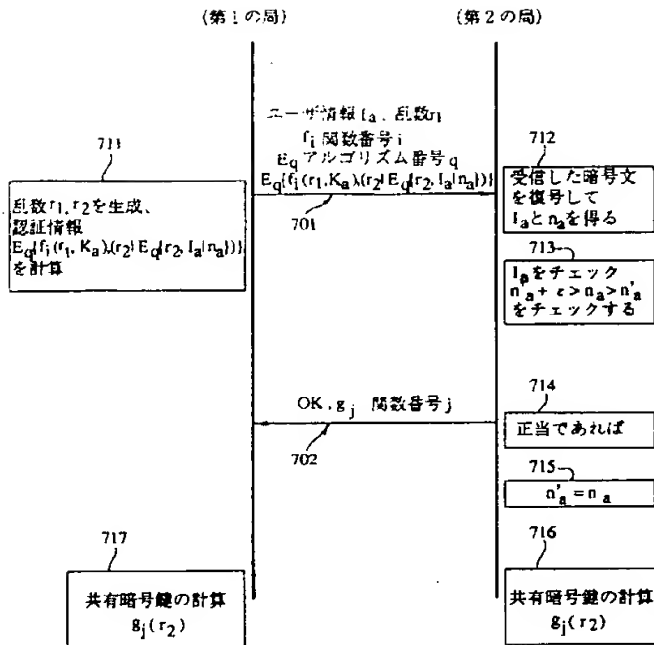
【図13】



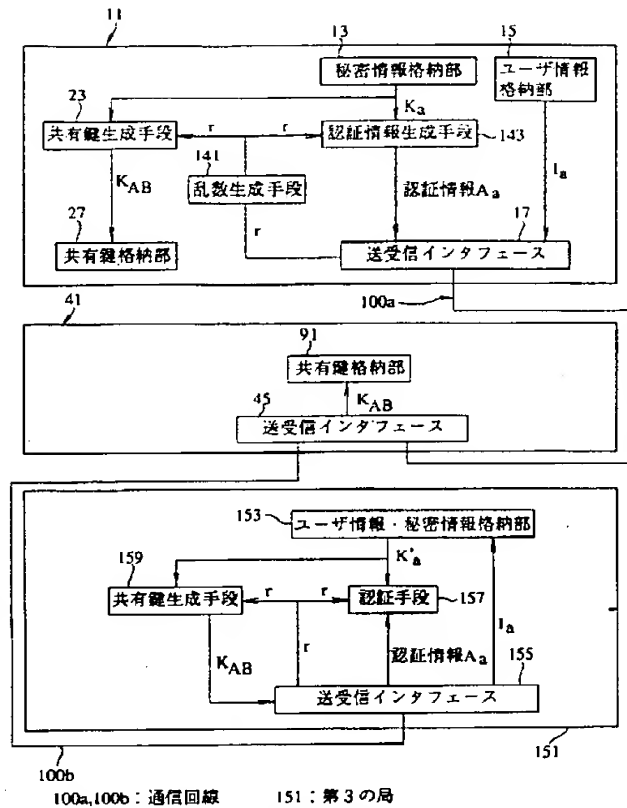
83: 認証手段

第7の実施の形態の通信システムの構成説明図

【図 15】

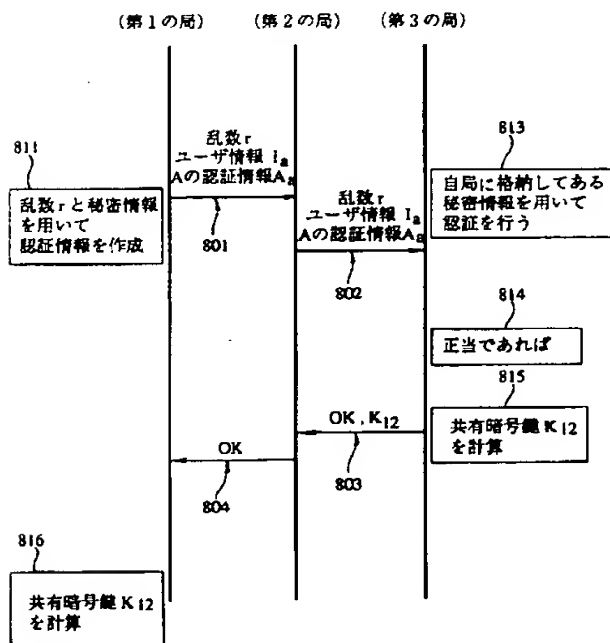


第7の実施の形態の通信システムの動作説明図



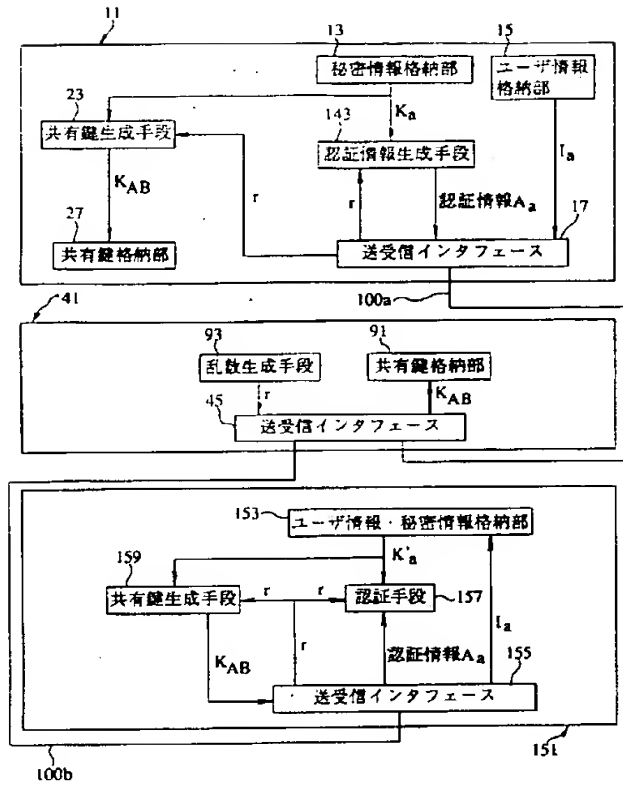
第8の実施の形態の通信システムの構成説明図

【图 16】



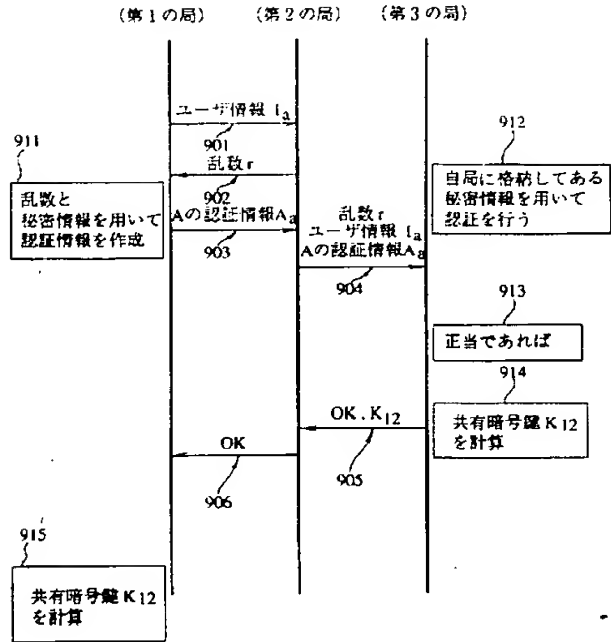
第8の実施の形態の通信システムの動作説明図

【図17】



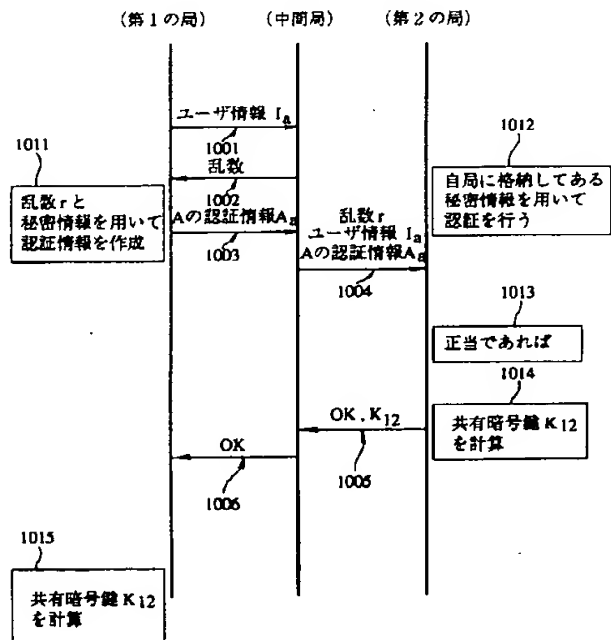
第9の実施の形態の通信システムの構成説明図

【図18】



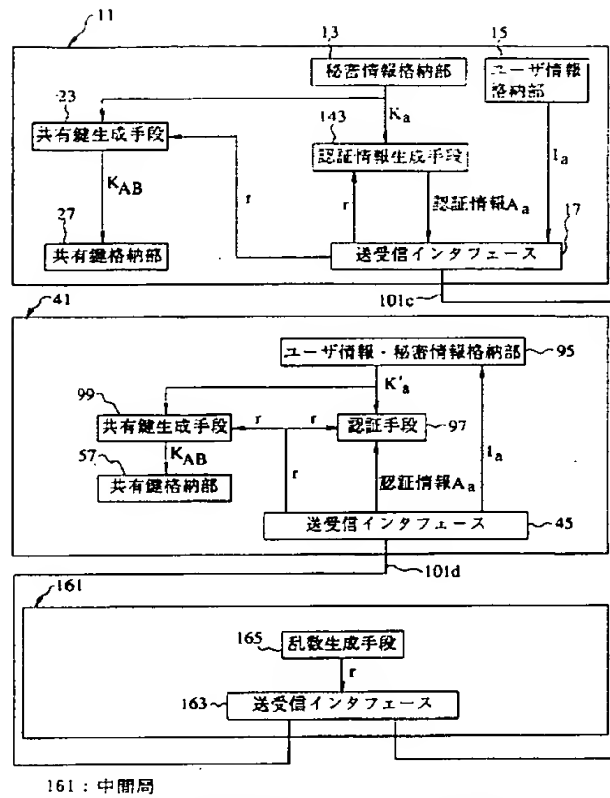
第9の実施の形態の通信システムの動作説明図

【図20】



第10の実施の形態の通信システムの動作説明図

【図19】



第10の実施の形態の通信システムの構成説明図

フロントページの続き

(72) 発明者 鳥居 肖史
 東京都港区虎ノ門1丁目7番12号 沖電気
 工業株式会社内